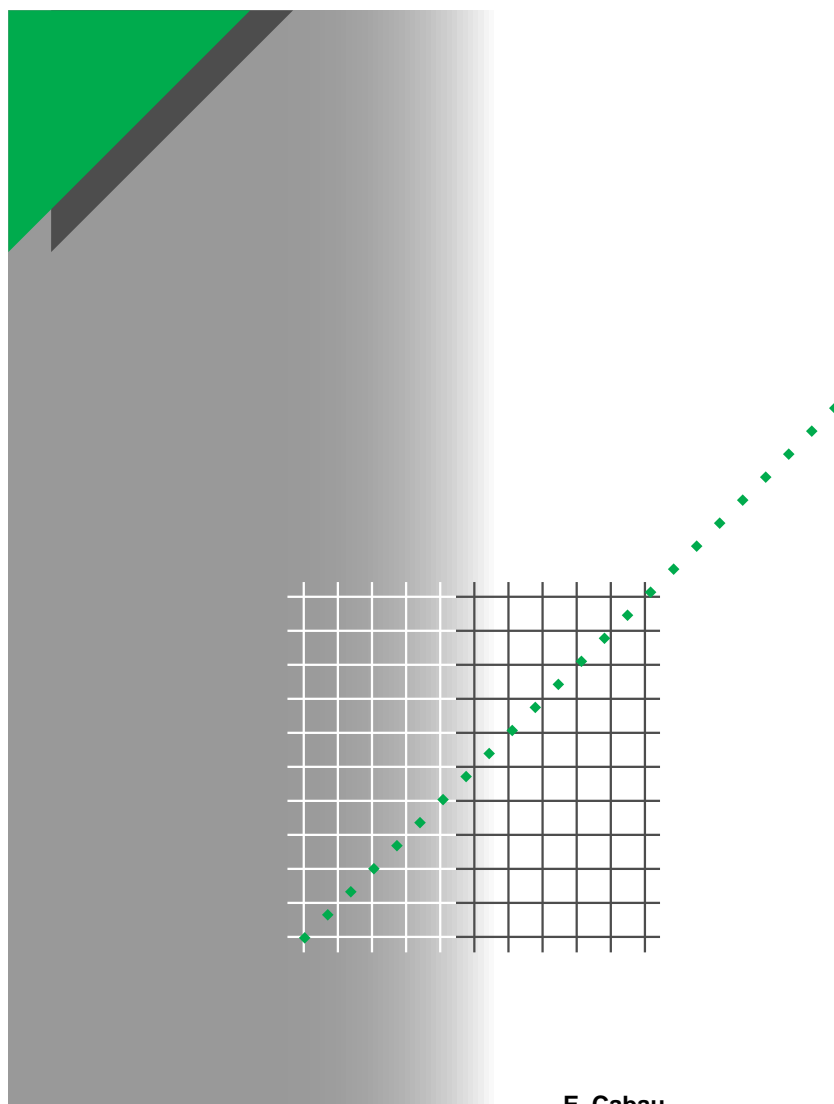


Cahier technique n° 144

Introduction à la conception de la sûreté



Merlin Gerin

Modicon

Square D

Telemecanique

E. Cabau

Les Cahiers Techniques constituent une collection d'une centaine de titres édités à l'intention des ingénieurs et techniciens qui recherchent une information plus approfondie, complémentaire à celle des guides, catalogues et notices techniques.

Les Cahiers Techniques apportent des connaissances sur les nouvelles techniques et technologies électrotechniques et électroniques. Ils permettent également de mieux comprendre les phénomènes rencontrés dans les installations, les systèmes et les équipements.

Chaque Cahier Technique traite en profondeur un thème précis dans les domaines des réseaux électriques, protections, contrôle-commande et des automatismes industriels.

Les derniers ouvrages parus peuvent être téléchargés sur Internet à partir du site Schneider Electric.

Code : <http://www.schneider-electric.com>

Rubrique : **Le rendez-vous des experts**

Pour obtenir un Cahier Technique ou la liste des titres disponibles contactez votre agent Schneider Electric.

La collection des Cahiers Techniques s'insère dans la « Collection Technique » de Schneider Electric.

Avertissement

L'auteur dégage toute responsabilité consécutive à l'utilisation incorrecte des informations et schémas reproduits dans le présent ouvrage, et ne saurait être tenu responsable ni d'éventuelles erreurs ou omissions, ni de conséquences liées à la mise en œuvre des informations et schémas contenus dans cet ouvrage.

La reproduction de tout ou partie d'un Cahier Technique est autorisée après accord de la Direction Scientifique et Technique, avec la mention obligatoire : « Extrait du Cahier Technique Schneider Electric n° (à préciser) ».

n° 144

Introduction à la conception de la sûreté

Emmanuel CABAU



Ingénieur ENSIMAG 1989 (INPG, Grenoble), est chez Schneider Electric depuis 1990.

Il se spécialise d'abord dans le domaine de plans d'expérience et techniques statistiques diverses auprès de la Direction Scientifique et Technique, puis, utilisant sa formation initiale d'informaticien, participe au développement d'un outil logiciel d'audit d'installation électrique pour Schneider Services.

En 1998, il rejoint le pôle de compétence des études de sûreté de fonctionnement, une équipe spécialisée dans l'étude de fiabilité de certains produits et process de Schneider Electric, notamment dans les domaines : contrôle-commande de centrales nucléaires, installations électriques, appareillage de coupure, système d'automatismes répartis, etc.

Introduction à la conception de la sûreté

La panne d'un équipement, l'indisponibilité d'une source d'énergie, l'arrêt d'un système automatique, l'accident sont de moins en moins tolérables et acceptés par le citoyen comme par l'industriel.

La sûreté qui se décline en terme de fiabilité, de maintenabilité, de disponibilité et de sécurité est maintenant une science qu'aucun concepteur de produit ou d'installation, ne peut ignorer.

Ce cahier technique vous propose une présentation des notions de base, et une explication des méthodes de calcul.

Quelques exemples et valeurs numériques permettent de faire contrepoids à quelques formules et à l'utilisation sous-jacente de nombreux outils informatiques.

Sommaire

1 L'importance de la sûreté	1.1 Dans le logement	p. 4
	1.2 Dans le tertiaire	p. 4
	1.3 Dans l'industrie	p. 4
2 Les grandeurs de la sûreté	2.1 Fiabilité	p. 5
	2.2 Taux de défaillance	p. 5
	2.3 Disponibilité	p. 6
	2.4 Maintenabilité	p. 7
	2.5 Sécurité	p. 7
3 Relations entre les grandeurs de la sûreté	3.1 Des grandeurs interactives	p. 8
	3.2 Des grandeurs qui peuvent s'opposer	p. 8
	3.3 Des grandeurs fonction des temps moyens	p. 9
4 Les types de défaut	4.1 Les défauts physiques	p. 11
	4.2 Les défauts de conception	p. 11
	4.3 Les défauts d'exploitation	p. 11
5 De l'élément au système : la modélisation	5.1 Les bases de données sur les composants des systèmes	p. 13
	5.2 La méthode APR	p. 15
	5.3 La méthode AMDEC	p. 16
	5.4 Les diagrammes de fiabilité	p. 16
	5.5 Les arbres de défaillance	p. 19
	5.6 Les graphes d'états	p. 22
	5.7 Les réseaux de Pétri	p. 24
	5.8 Choix d'une technique de modélisation	p. 25
6 Maintenance et logistique : de plus en plus complexe...	6.1 Optimisation de la maintenance par la fiabilité (O.M.F)	p. 26
	6.2 Soutien logistique intégré (S.L.I)	p. 26
7 Conclusion		p. 27
Bibliographie et normes		p. 28

1 L'importance de la sûreté

L'homme des cavernes devait être sûr de son bras. L'homme moderne est entouré d'outils, de systèmes de plus en plus sophistiqués dont il

doit être sûr, ceci s'il veut qu'ils concourent réellement à sa sécurité, son efficacité et son confort.

1.1 Dans le logement

Le citoyen, dans sa vie de tous les jours, est fortement intéressé par :

- la fiabilité de son téléviseur,
- la disponibilité de l'électricité,

- la réparabilité de son congélateur ou de sa voiture,
- la sécurité du coupe-gaz de sa chaudière.

1.2 Dans le tertiaire

Le banquier et tout le secteur tertiaire accorde beaucoup d'importance à :

- la fiabilité de l'informatique,
- la disponibilité du chauffage,

- la réparabilité des ascenseurs,
- la sécurité incendie.

1.3 Dans l'industrie

L'industriel qui doit être compétitif ne peut admettre de pertes de production, d'autant plus importantes que son processus de fabrication est complexe ; il recherche la meilleure :

- fiabilité de ses systèmes contrôle commande,
- disponibilité de ses machines,
- maintenabilité de l'outil de production,
- sécurité des personnes et du capital industriel.

Ces valeurs que l'on regroupe sous le concept de SURETE (être sûr) font appel à la notion de confiance. Elles se quantifient en terme d'objectif, se calculent en terme de probabilité,

se réalisent en terme d'architecture et de choix de composants, se vérifient par les tests ou l'expérience.

Schneider Electric intègre ce concept de sûreté de longue date. Il en est ainsi, entre autres, depuis 30 ans pour les produits Merlin Gerin dont on connaît la contribution : hier, par exemple, à la conception des centrales nucléaires, ou à l'exceptionnelle disponibilité de l'énergie électrique de la base de lancement des fusées ARIANE, aujourd'hui dans la conception des produits et systèmes destinés à tous les secteurs d'activité.

2 Les grandeurs de la sûreté

2.1 Fiabilité

L'ampoule électrique est utile au particulier, au banquier et à l'industriel. Quand ils l'allument ils veulent tous qu'elle éclaire jusqu'à ce qu'ils l'éteignent !

La fiabilité est la probabilité que l'ampoule soit en état de fonctionner à l'instant t, elle mesure l'aptitude à rester dans un état de fonctionnement correct.

Définition : la fiabilité est la probabilité pour qu'une entité puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné $[t_1, t_2]$; que l'on écrit : $R(t_1, t_2)$.

Cette définition, celle de la CEI (Commission Electrotechnique Internationale), est donnée dans la norme 191 de juin 1988.

Plusieurs notions sont fondamentales dans cette définition :

- **Fonction** : la fiabilité est caractéristique de la fonction attribuée au système. La connaissance de son architecture matérielle est souvent insuffisante et il faut utiliser des méthodes d'analyse fonctionnelle.
- **Conditions** : le rôle de l'environnement est primordial en fiabilité, il faut aussi connaître les conditions d'utilisation. La connaissance du matériel n'est pas suffisante.
- **Intervalle** : on s'intéresse à une durée et pas à un instant. Par hypothèse le système fonctionne à l'instant initial, le problème est de savoir pour combien de temps. En général $t_1 = 0$ et on note $R(t)$ la fiabilité.

2.2 Taux de défaillance

Conservons l'exemple de l'ampoule. Son taux de défaillance à l'instant t, noté $\lambda(t)$, mesure la probabilité qu'elle s'éteigne intempestivement dans l'intervalle $[t, t+\Delta t]$ sachant qu'elle est restée allumée jusqu'à l'instant t. Le taux de défaillance est un taux horaire qui est homogène à l'inverse d'un temps.

L'écriture mathématique est la suivante :

$$\begin{aligned}\lambda(t) &= \lim_{\Delta t \rightarrow 0} \left(\frac{1}{\Delta t} \cdot \frac{R(t) - R(t + \Delta t)}{R(t)} \right) \\ &= -1 \cdot \frac{dR(t)}{dt} \quad (1)\end{aligned}$$

Ainsi, le taux de défaillance qui mesure la probabilité pour une personne âgée de 20 ans de mourir dans l'heure qui suit se note :

$\lambda(20 \text{ ans}) = 10^{-6}$ par heure.

Si on représente λ en fonction de l'âge on obtient alors une courbe qui est celle de la **figure 1**.

Après de fortes valeurs qui correspondent à la mortalité infantile, λ atteint la valeur de l'âge adulte durant laquelle il est constant car les causes de décès sont surtout accidentelles et donc indépendantes de l'âge. A partir de 60 ans,

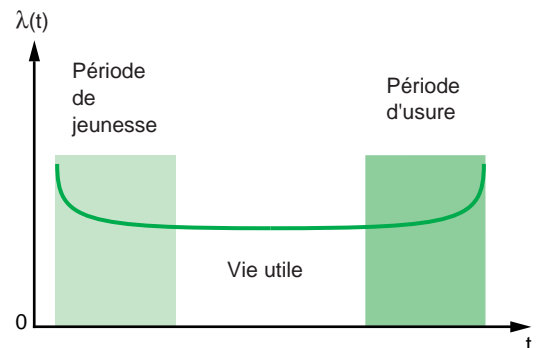


Fig. 1 : courbe en baignoire.

du fait du vieillissement λ augmente. L'expérience a montré que pour les composants électroniques la courbe obtenue a la même allure, d'où la terminologie : période de jeunesse, vie utile et période d'usure.

Pendant la période de vie utile le taux λ est constant et l'équation (1) donne : $R(t) = \exp(-\lambda t)$. La loi est dite **exponentielle**, la courbe de fiabilité en fonction du temps, dans ce cas, est celle de la **figure 2**. La loi exponentielle est une des lois possibles. Les dispositifs mécaniques soumis, dès le début

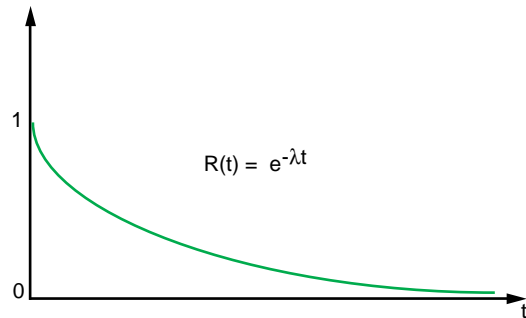


Fig. 2 : fiabilité exponentielle.

de leur emploi, à l'usure peuvent suivre une autre loi, par exemple la loi de Weibull, dans laquelle le taux de défaillance est fonction du temps. Si on trace la courbe donnant λ en fonction du temps on obtient alors une courbe qui n'a pas le plateau de la figure 1 (cf. **figure 3**).

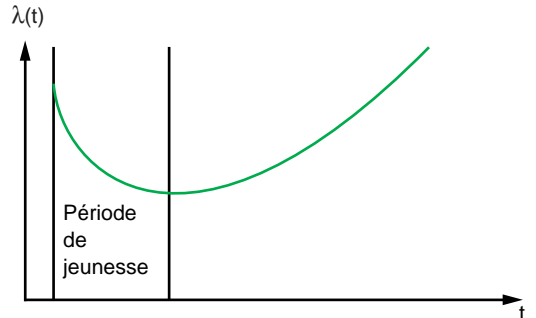


Fig. 3 : courbe de fiabilité avec usure.

2.3 Disponibilité

La notion de disponibilité s'illustre très bien avec celle d'un véhicule. Une voiture doit fonctionner à l'instant du besoin, l'historique importe peu. La disponibilité mesure cette aptitude à fonctionner à un instant donné.

Définition : la disponibilité est la probabilité pour qu'une entité soit en état d'accomplir une fonction requise dans des conditions données à un instant donné t , en supposant que la fourniture des moyens extérieurs nécessaires est assurée. On la note : $D(t)$.

Cette définition de la CEI est calquée sur celle de la fiabilité mais l'aspect temporel est fondamentalement différent puisqu'on s'intéresse à un état à un instant donné et pas à une durée.

Le fonctionnement à l'instant t ne nécessite pas forcément le fonctionnement sur $[0, t]$ pour un système réparable. C'est là que se situe la différence fondamentale avec la fiabilité.

On peut tracer la courbe donnant la disponibilité en fonction du temps d'un élément réparable dans le cas de lois exponentielles pour les défaillances et les réparations (cf. **figure 4**).

On constate que la disponibilité tend vers une valeur limite qui est, par définition, la disponibilité asymptotique. Cette valeur limite est atteinte au bout d'un temps qui est de l'ordre du temps de

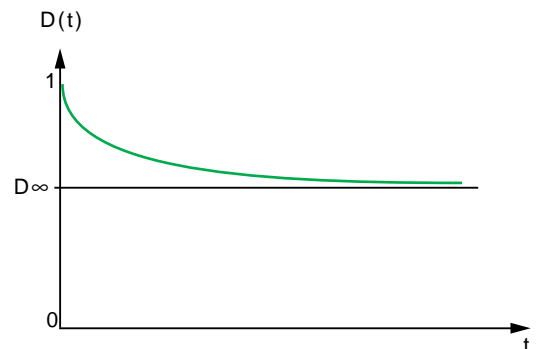


Fig. 4 : disponibilité en fonction du temps.

réparation. La fiabilité a toujours une limite nulle puisqu'aucun système n'est éternel. (Ce dernier point peut être contesté dans le cas des logiciels).

Revenons sur l'exemple de la voiture. Deux types de véhicules posent des problèmes de disponibilité : ceux qui tombent souvent en panne et ceux qui, bien que rarement en panne, restent longtemps au garage avant d'être réparés. La fiabilité participe donc à la disponibilité mais l'aptitude à être réparée rapidement est aussi importante, c'est la maintenabilité.

2.4 Maintenabilité

Les concepteurs recherchent toujours la performance maximum du produit et négligent parfois l'hypothèse de la panne. Il est difficile quand on fait tout pour que le système fonctionne de se demander ce qu'il adviendra en cas de panne. Pourtant cette interrogation est indispensable. Pour qu'un système soit disponible, il doit défaillir le plus rarement possible mais il est tout aussi important qu'il soit très rapidement réparé. On entend ici par réparation l'ensemble de la remise en service incluant les délais logistiques. L'aptitude d'un système à être réparé est mesurée par la maintenabilité.

Définition : la maintenabilité est la probabilité pour qu'une opération donnée de maintenance active puisse être effectuée pendant un intervalle de temps donné $[t_1, t_2]$; que l'on écrit : $M(t_1, t_2)$. Cette définition est également extraite du vocabulaire international normalisé par la CEI. Elle traduit que la maintenabilité est à la réparation ce que la fiabilité est à la défaillance. On définit avec les mêmes hypothèses que pour $R(t)$ la maintenabilité $M(t)$. Le taux de réparation $\mu(t)$ est introduit de façon similaire au taux de défaillance - voir ce paragraphe ci-dessus, équation (1). Lorsqu'il est constant, la loi est exponentielle et on a : $M(t) = \exp(-\mu t)$.

2.5 Sécurité

On distingue les pannes dangereuses des pannes non dangereuses. La différence ne réside pas dans la nature des pannes mais dans leurs conséquences. Le fait d'éteindre tous les feux dans une gare ou de les faire passer intempestivement du vert au rouge affecte le fonctionnement (arrêt des trains) mais n'est pas directement dangereux. Cela est complètement différent dans le cas où les feux passeraient du rouge au vert.

La sécurité est la probabilité d'éviter un événement dangereux.

La notion de sécurité est étroitement liée à celle du risque qui lui-même dépend non seulement de la probabilité d'occurrence mais aussi de la gravité de l'événement. On peut accepter de risquer sa vie, grande gravité, si la probabilité d'occurrence est assez faible. Si le risque est uniquement de se casser une jambe on peut accepter une probabilité plus grande. La courbe de la **figure 5** illustre le concept de risque acceptable.

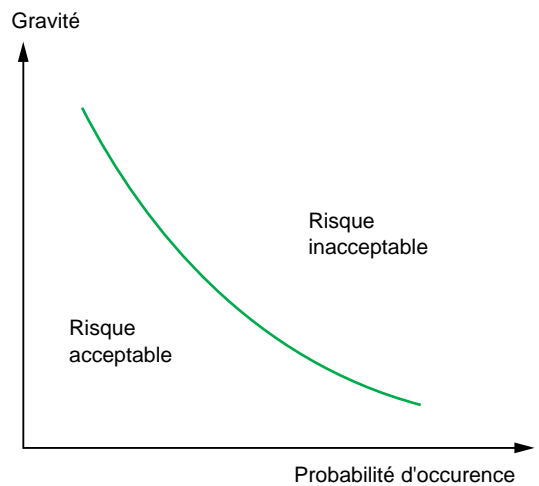


Fig. 5 : le niveau de risque est fonction du couple : gravité, probabilité d'occurrence.

3 Relations entre les grandeurs de la sûreté

3.1 Des grandeurs interactives

A travers ces quelques exemples on voit que la SURETE est un concept qui se décline en 4 grandeurs chiffrables ; elles dépendent les unes des autres (cf. **figure 6**).

Ces quatre grandeurs sont à prendre en compte pour toute étude de sûreté.

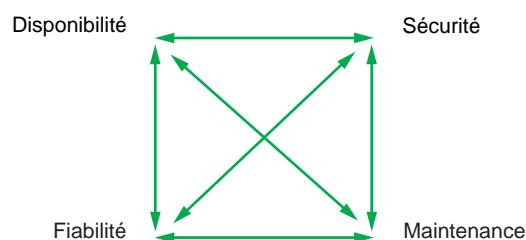


Fig. 6 : les composantes de la sûreté.

On désigne parfois la sûreté par les initiales de ses quatre grandeurs caractéristiques, FMDS :

- **F**iability : probabilité que le système soit non défaillant sur $[0,t]$.
- **M**aintainability : probabilité que le système soit réparé sur $[0,t]$.
- **D**isponibility : probabilité que le système fonctionne à l'instant t .
- **S**ecurity : probabilité d'éviter un événement catastrophique.

La correspondance avec la terminologie anglaise est la suivante :

- Fiabilité : Reliability.
- Maintenabilité : Maintainability.
- Disponibilité : Availability.
- Sécurité : Safety.
- Sûreté de fonctionnement : Dependability.

3.2 Des grandeurs qui peuvent s'opposer

Parmi les grandeurs caractéristiques de la sûreté certaines peuvent être contradictoires.

L'amélioration de la maintenabilité peut amener à des choix qui dégradent la fiabilité (par exemple adjonction de composants pour faciliter le montage-démontage). La disponibilité est donc un compromis entre la fiabilité et la maintenabilité ; une étude de sûreté permet de chiffrer ce compromis.

De même, la sécurité et la disponibilité peuvent être contradictoires.

On a vu que la sécurité est la probabilité d'éviter un événement dangereux, elle est souvent maximum quand le système est arrêté, mais la disponibilité est alors nulle : c'est le cas lorsqu'on ferme à la circulation un pont risquant de s'effondrer. A l'inverse pour améliorer la disponibilité de leurs appareils certaines compagnies aériennes peuvent être tentées de négliger la maintenance préventive et la sécurité en vol diminue. La détermination d'un système répondant au compromis optimal entre la sécurité et la disponibilité impose de pouvoir calculer ces grandeurs.

Un système peut occuper trois états, (cf. **figure 7**). Outre l'état de fonctionnement normal on considère deux états de panne : l'un dangereux et l'autre pas. Dans un but de simplification les états de panne incluent tous les fonctionnements dégradés, d'où la désignation « fonctionnement incorrect ».

Le temps écoulé avant de quitter l'état A est caractéristique de la fiabilité. Le temps passé dans l'état B après une panne « sûre » est caractéristique de la maintenabilité. Le ratio entre le temps passé dans l'état A et le temps total est caractéristique de la disponibilité. L'aptitude du système à ne pas transiter vers l'état C est caractéristique de la sécurité. On constate que l'état B est performant vis-à-vis de la sécurité ; mais il est source d'indisponibilité.

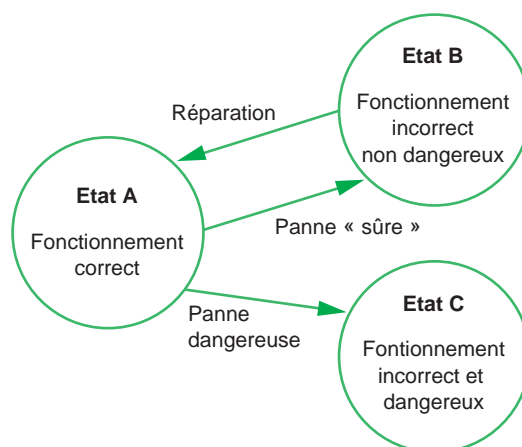


Fig. 7 : panne sûre : disponibilité !
panne dangereuse : sécurité !

3.3 Des grandeurs fonction des temps moyens

Outre les probabilités (fiabilité, maintenabilité, disponibilité, sécurité) d'occurrence d'événements introduites dans ce qui précède, on utilise aussi les temps moyens avant l'occurrence d'événements pour caractériser la sûreté.

Les temps moyens

Il est utile de rappeler la définition précise de tous les temps moyens car ils sont souvent mal utilisés. Le plus mal utilisé est peut-être le plus connu, le MTBF, qui est souvent considéré à tort comme une durée de vie. En effet au bout d'un temps égal au MTBF, si la loi est exponentielle, et pour une population homogène, presque 2/3 des dispositifs, en moyenne, sont défectueux. S'il s'agit d'un système, celui-ci a 63 % de chances d'avoir eu une panne. Les définitions et le positionnement de ces temps moyens situés au

cours de la vie d'un système sont rappelés **figure 8**.

MTTF ou MTFF (Mean Time To First Failure) : temps moyen de bon fonctionnement avant la première défaillance.

MTBF (Mean Time Between Failure) : temps moyen entre deux défaillances d'un système réparable.

MDT (Mean Down Time) : durée moyenne de défaillance comprenant la détection de la panne, la durée d'intervention, le temps de la réparation et le temps de remise en service.

MTTR (Mean Time To Repair) : temps moyen de réparation.

MUT (Mean Up Time) : durée moyenne de bon fonctionnement après réparation.

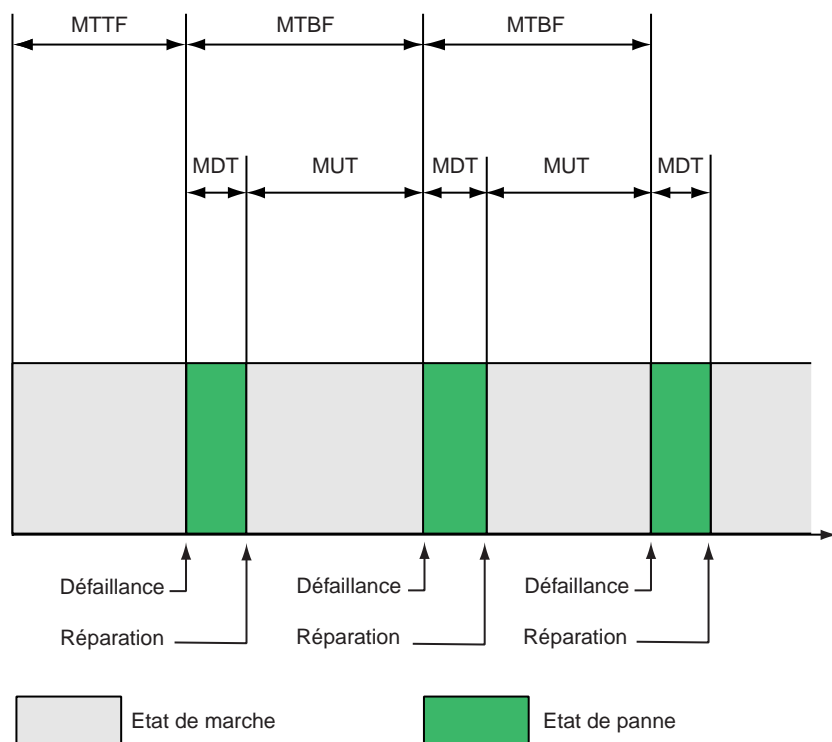


Fig. 8 : diagramme des temps moyens, établi pour un système ne nécessitant pas d'interruption de fonctionnement pour maintenance préventive.

Quelques relations et valeurs numériques

Il existe de nombreuses relations entre les grandeurs introduites.
 Pour une loi exponentielle $R(t) = \exp(-\lambda t)$,
 $MTTF = 1/\lambda$; or pour un système non réparable
 $MTBF = MTTF$ (en effet toutes les pannes sont
 alors des premières pannes). Ceci explique la
 formule classiquement utilisée pour les
 composants électroniques (non réparables) :
 $MTBF = 1/\lambda$.
 Il ne faut appliquer cette formule que pour des
 lois exponentielles et, en toute rigueur, pour un
 composant non réparable (on peut s'affranchir
 de cette dernière hypothèse si la MDT est
 suffisamment faible).

Lorsque les temps de réparations suivent aussi
 une loi exponentielle on montre de même que
 $MTTR = 1/\mu$.

On a $MTBF = MUT + MDT$. En général
 $MDT = MTTR$ mais il faut parfois ajouter les
 délais logistiques ou de démarrage.

On a de plus :

■ disponibilité asymptotique

$$D_{\infty} = \lim_{t \rightarrow +\infty} (D(t))$$

$$= \frac{MUT}{MDT + MUT} = \frac{MUT}{MTBF}$$

Cette formule illustre l'interprétation de la
 disponibilité donnée en page 5 (ratio du temps
 de bon fonctionnement par rapport au temps
 total). Cette valeur ($MUT/MTBF$) correspond à
 l'asymptote de la figure 4.

■ indisponibilité asymptotique = 1 - disponibilité asymptotique

$$ID_{\infty} = \lim_{t \rightarrow +\infty} (1 - D(t))$$

$$= \frac{MDT}{MDT + MUT} = \frac{MDT}{MTBF}$$

L'indisponibilité asymptotique est en général
 plus facile à exprimer numériquement que la
 disponibilité (on lit plus facilement 10^{-6} que
 0,999999).

Pour des lois exponentielles avec les relations
 $MUT = 1/\lambda$ et $MDT = 1/\mu$ on arrive à :

$$ID_{\infty} = \frac{\lambda}{\lambda + \mu} \quad \text{ou} \quad D_{\infty} = \frac{\mu}{\lambda + \mu}$$

λ est souvent négligeable devant μ puisque le
 temps de réparation est petit devant le temps
 moyen avant panne. On peut donc simplifier le
 dénominateur et on obtient :

$$ID_{\infty} = \frac{\lambda}{\mu} = \lambda \cdot MTTR$$

Cette dernière formule chiffre dans le cas de lois
 exponentielles le compromis fiabilité-
 maintenabilité qu'il faut optimiser pour améliorer
 la disponibilité.

Le tableau ci-après (cf. fig.9) donne un ordre de
 grandeur du taux de défaillance et du temps
 moyen avant la première panne pour un certain
 nombre d'éléments des domaines électronique
 et électrotechnique.

On constate bien sûr que la fiabilité se dégrade
 quand la complexité augmente. Ceci correspond
 d'ailleurs à une règle de base de la conception
 de la sûreté : faire simple autant que possible.
 La notion de temps moyen est souvent mal
 comprise. Les deux phrases suivantes signifient
 la même chose dans le cas d'une loi
 exponentielle :

« Le MTTF vaut 100 ans » et « on a une chance
 sur 100 d'observer une panne la première
 année ». Cette deuxième phrase semble
 pourtant plus inquiétante pour un industriel qui
 vend 10 000 appareils de ce type chaque année.
 En moyenne une centaine d'appareils tomberont
 en panne la première année.

Pour l'indisponibilité on peut citer comme
 exemple le réseau électrique national. On
 s'intéresse à la présence d'énergie électrique
 conforme à l'attente de l'utilisateur.

L'indisponibilité est de l'ordre de 10^{-3} ce qui
 correspond en moyenne à 9 heures de panne
 par an. Pour une salle informatique entièrement
 secourue par un ensemble d'onduleurs
 fortement redondants on peut atteindre une
 disponibilité 1 000 ou 10 000 fois meilleure.

	Résistances	Micro processeur	Fusible et disj. forte intensité, transfos, câbles (100 m) jeu de barres (10 départs)	Générateur	Coupures brèves EDF
λ (/h)	10^{-9}	10^{-6}	entre 10^{-7} et 10^{-6}	10^{-5}	10^{-3}
MTTF	1000 siècles	100 ans	entre 100 et 1000 ans	10 ans	40 jours

Fig. 9 : taux de défaillance et MTTF de quelques éléments.

4 Les types de défaut

La réalisation d'un système satisfaisant à un objectif de sûreté nécessite d'identifier et prendre en compte les causes possibles de défauts. La classification suivante peut être proposée :

Les défauts physiques

Ils peuvent être induits par des causes **internes** (rupture d'un élément) ou **externes** (interférences électro-magnétiques, vibrations...).

Les défauts de conception

Ils regroupent notamment les erreurs de conception matérielles et les erreurs logicielles.

Les défauts d'exploitation

Ils désignent les défauts engendrés par une mauvaise utilisation du matériel :

- utilisation du matériel dans un environnement pour lequel il n'a pas été conçu,
- erreur d'un opérateur humain dans l'utilisation du matériel ou lors d'une opération de maintenance,
- malveillance.

Les techniques développées dans ce document concernent prioritairement la prise en compte des défauts physiques.

Cependant, le problème des erreurs humaines et des erreurs logicielles n'est pas à négliger, même si l'état de l'art dans ces domaines est moins riche que pour les défauts physiques. Nous nous contenterons de mentionner, dans le cadre de ce cahier technique, les éléments de réflexions suivants.

En matière de logiciels :

- Le logiciel ignore le phénomène de vieillissement, mais dès qu'il est complexe, il est nécessaire de valider sa conception par une démarche sûreté.
- Cette démarche intervient à la fois en phase de conception et en phase de validation.
- La première étape de la démarche peut-être l'Analyse des Effets des Erreurs du Logiciel (AEEL) qui identifie les parties critiques et préconise des actions de conception ou de validation. Mais cette analyse est souvent trop lourde pour être menée dans le détail.

■ En conception sont utilisés des ateliers logiciels adaptés à la sûreté (chez Schneider Electric, LUSTRE et SCADE, par exemple) et des techniques de redondance (plusieurs versions du même logiciel développées indépendamment).

■ En validation sont utilisées les techniques d'inspection formelle et de preuve de propriété.

■ Quantifier de façon exacte la fiabilité d'un logiciel reste difficile. Les meilleurs résultats sont atteints pour des études préliminaires effectuées pour des environnements (langage, méthode) précis. C'est le cas au sein de Schneider Electric où a été développé, par exemple, les logiciels pilotant le cœur des centrales nucléaires : SPIN (Système de Protection Intégré Numérique).

■ Schneider Electric participe à un groupe de travail européen sur la sûreté du logiciel (voir bibliographie).

La fiabilité humaine

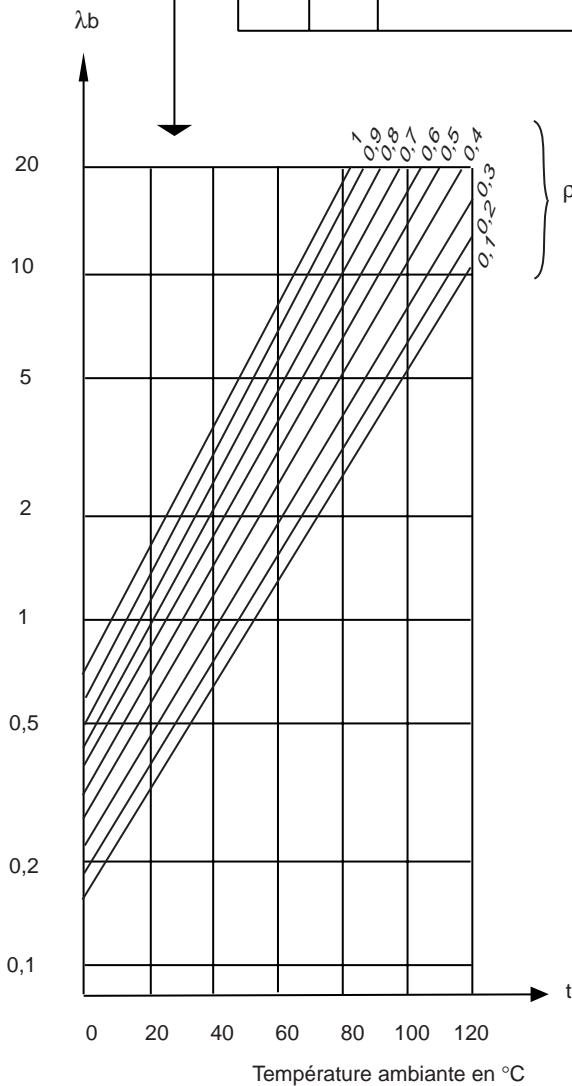
L'aspect qualitatif prévaut dans ce domaine. L'effort porte sur la schématisation de l'opérateur humain et sur la classification des tâches et des erreurs humaines. Les études les plus poussées sont celles réalisées dans le domaine nucléaire. Le comportement de l'opérateur est connu à la fois par des simulateurs et par les retours d'expérience, les deux sources peuvent être confrontées.

La littérature américaine fournit même des valeurs numériques qui sont à utiliser avec précaution : selon le type d'action (machinales, procédurales, cognitives) on évalue la probabilité d'erreur.

Les événements actuels en particulier les grandes catastrophes, montrent que les défaillances humaines sont une cause essentielle non seulement au niveau de l'opérateur mais aussi au niveau du concepteur. Plus la liberté d'action de l'homme est grande plus les risques encourus sont importants. L'accident de la navette américaine en 1987 montre que même le management de projet peut être en cause : on remonte jusqu'aux concepteurs de la structure de travail des concepteurs de la navette ! Les compétences multiples sont nécessaires pour aborder le problème de la fiabilité humaine, en particulier la psychologie et l'ergonomie.

RÉSISTANCES FIXES AGGLOMÉRÉES

$$\lambda = \lambda_b \cdot \pi_R \cdot \pi_E \cdot \pi_Q \cdot 10^{-9}/h$$



λ_b en fonction de la température ambiante t et du facteur de charge ρ

CCTU 04 01 A
modèle RA

MIL - R - 11 (RC)
MIL - R - 39 008 (RCR)

Informations nécessaires

Température ambiante	t	π_R π_E π_Q	
Dissipation effective	}		ρ
Dissipation nominale			
Valeur de la résistance	R		
Environnement			
Classes de qualification			

Facteur de charge ρ

$$\rho = \frac{\text{Dissipation effective}}{\text{Dissipation nominale}}$$

Classes de qualification

		π_Q
Agrément (PTT, ...)	avec CCQ	0,5
	sans CCQ	1
CCQ (UTE/CECC)	sauf usage général	1
	usage général	2,5
Homologation		2,5
Qualification par un client		5
Sans qualification (produit courant)		7,5

Environnement

	π_E
Au sol (conditions favorables)	1
Au sol (matériel fixe)	2,9
Au sol (matériel mobile)	8,3
Satellite en orbite	1
Missile (lancement)	29
Avion de transport (zones habitables)	2,8
Avion de transport (zones non habitables)	5,7
Avion de combat (zones habitables)	5,7
Avion de combat (zones non habitables)	11
Bateau (zones protégées)	5,2
Bateau (zones non protégées)	12

Valeur de la résistance

	π_R
$R \leq 100 \text{ k}\Omega$	1
$0,1 \text{ M}\Omega < R \leq 1 \text{ M}\Omega$	1,1
$1 \text{ M}\Omega < R \leq 10 \text{ M}\Omega$	1,6
$R > 10 \text{ M}\Omega$	2,5

Répartition des défauts

Courts-circuits :	0%
Circuits ouverts :	100%

Modèle mathématique

$$\lambda_b = 9 \cdot 10^{-6} \cdot e^{\left[12 \left(\frac{t+273}{343} \right) + \left(\frac{\rho}{0,6} \right) \left(\frac{t+273}{273} \right) \right]}$$

Fig. 10 : exemple de feuille de calcul issue des cahiers du CNET.

5 De l'élément au système : la modélisation

5.1 Les bases de données sur les composants des systèmes

On utilise le plus souvent les bases de données décrites ci-après, mais il est préférable, quand cela est possible de recueillir les données de retours d'expériences auprès des constructeurs des composants que l'on utilise. Cependant, ces données sont difficiles à obtenir car tous les constructeurs ne s'efforcent pas de les collecter systématiquement ou bien elles sont conservées confidentiellement.

En électronique

Dans ce domaine la fiabilité est très pratiquée depuis de nombreuses années. Les deux bases de données les plus utilisées sont le Military Handbook 217 (F, notice 2), américain, et le recueil de fiabilité du Centre National d'Etudes des Télécommunications (CNET) (cf. **figure 10**). Schneider Electric participe à sa mise à jour.

Ces recueils permettent de calculer le taux de défaillance supposé constant d'un composant en fonction des caractéristiques de l'application, (environnement ou taux de charge par exemple), ainsi que du type de composant, (nombre de portes, valeur de la résistance).

Prenons par exemple une résistance de 50 k Ω sur une carte électronique placée dans un tableau électrique.

On consulte les tableaux de la page 10 pour déterminer les différents facteurs correctifs.

L'environnement est « Au sol (matériel fixe) », le facteur multiplicatif relatif à l'environnement est donc :

$$\Pi_E = 2,9.$$

La valeur de la résistance donne le facteur multiplicatif correspondant :

$$\Pi_R = 1.$$

La résistance est sans qualification ce qui donne le facteur multiplicatif relatif au facteur de qualité :

$$\Pi_Q = 7,5.$$

Le facteur de charge ρ est caractéristique de l'application contrairement aux autres facteurs qui sont caractéristiques du composant. Si le facteur de charge est de 0,7 et la température ambiante pour la carte est de 90° C. L'abaque donne $\lambda_b = 15$.

On obtient alors le taux de défaillance de la résistance en effectuant le produit :

$$\lambda = \lambda_b \cdot \Pi_R \cdot \Pi_E \cdot \Pi_Q \cdot 10^{-9} = 0,33 \cdot 10^{-6}.$$

Si la conception est réalisée en intégrant l'objectif fiabilité :

■ Des échanges thermiques mieux étudiés permettent d'abaisser la température ambiante.

■ Une meilleure conception de la carte électronique permet de diminuer le facteur de charge ρ .

Avec $t = 60^\circ \text{C}$ et $\rho = 0,2$ l'abaque donne $\lambda_b = 1,7$.

Si on prend un composant homologué : $\Pi_Q = 2,5$ on obtient alors : $\lambda = 0,012 \cdot 10^{-6}$ soit un gain d'un facteur 30.

Connaissant la fiabilité de chaque composant on passe facilement à la fiabilité des cartes, (qui sont réparables ou remplaçables), puis des systèmes électroniques en utilisant les méthodes de modélisation décrites dans la suite de ce chapitre 5.

Remarques importantes :

■ L'exemple ci-dessus est purement illustratif pour montrer l'esprit des calculs de fiabilité en électronique. Les valeurs numériques et les paramètres utilisés sont en constante évolution et régulièrement mis à jour.

■ C'est d'ailleurs la raison pour laquelle depuis plusieurs années déjà, les calculs sont effectués à partir d'outils logiciels. Le plus connu est RELEX et il réunira à partir de 1999 les deux bases de données du Military Handbook et du CNET.

En électrotechnique et en mécanique

Les recueils de données existants sont moins reconnus qu'en électronique, mais ils sont très utilisés.

On peut citer :

■ RAC NPRD 95 : rapport du Reliability Analysis Center, organisme militaire américain, concernant les composants et dispositifs non électroniques.

■ IEEE STD 493 : recueil de données de fiabilité observées et concernant des équipements électriques dans les installations électriques industrielles.

■ IEEE STD 500 : recueil de données de fiabilité observées et concernant des équipements électriques, électroniques et mécaniques installés dans les centrales nucléaires.

On utilise aussi des ouvrages de référence qui contiennent des méthodes de calcul et des données propres à certains domaines. Par exemple l'ouvrage de Cl. Marcovici et J. Cl. Ligeron : « Utilisation des techniques de fiabilité en mécanique ».

A titre d'illustration, la **figure 11** donne un extrait du RAC NPRD97 concernant les disjoncteurs. On a tout d'abord une répartition des différents modes de défaillances, on lit par exemple que 34 % des défaillances constatées sont des refus de fermeture. Le tableau de la figure 9 donne une estimation de la valeur du taux de défaillance (point estimate) en ce qui concerne la fonction thermique (thermal) des disjoncteurs.

On lit successivement :

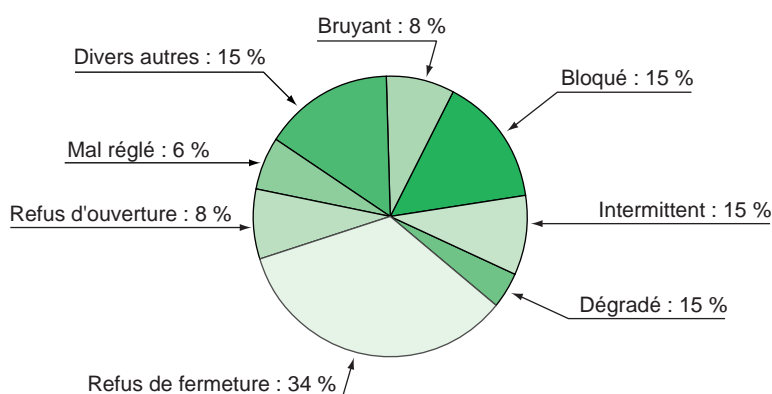
- l'environnement : ici GF = Ground Fixed = au sol conditions industrielles,
- l'estimation du taux de défaillance : il faut lire $0,335 \cdot 10^{-6} \text{ h}^{-1}$,
- les bornes d'un intervalle de confiance tel que la probabilité que le taux de défaillance s'y trouve est de 0,6 (c'est-à-dire 0,8 - 0,2),
- le nombre de recueils utilisés pour le calcul : ici 2,
- le nombre de défaillances observées : ici 3,
- le nombre d'heures de fonctionnement observées : $8,944 \cdot 10^6 \text{ h}$.

La connaissance du taux de défaillance global et de la répartition par mode de défaillance permet de chiffrer la probabilité des différents événements par une simple règle de trois. Par exemple, pour le mode de défaillance « refus de fermeture », on obtient :

$$0,335 \cdot 10^{-6} \times \frac{34}{100} = 1,17 \cdot 10^{-7}$$

Une autre approche est parfois plus pertinente : on considère un nombre de manœuvres au lieu de considérer le temps de fonctionnement. Dans ce cas un test portant sur un échantillon de quelques dizaines de produits permet de chiffrer la fiabilité (loi de Weibull).

Le choix dépend du type de défaillances que l'on désire étudier, l'usure des contacts est liée au nombre de manœuvres alors que la corrosion est liée au temps. Le type d'utilisation et les conditions d'environnement sont toujours déterminants.



Component part type	APPL ENV	User code	Point estimate	60 % upper single-side	20 % lower internal	80 % upper internal	% of recs	% of fail	Operating HRS (E6)
Thermal	GF	M	0,335	-	0,171	0,621	2	3	8,944

Fig. 11 : mode de défaillances et données de fiabilité des disjoncteurs.

5.2 La méthode APR

Une APR est une Analyse Préliminaire des Risques qui a pour objectif d'identifier les dangers d'une installation industrielle et ses causes (exemples : entités dangereuses, situations dangereuses accidents potentiels). Elle peut comporter également une évaluation de la gravité des conséquences liées aux situations dangereuses et aux accidents potentiels.

A faire dès les premières phases de la conception et à remettre à jour au fur et à mesure du déroulement du projet, cette analyse permet de déduire tous les moyens, toutes les actions correctrices permettant d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels.

Elle ne doit pas être confondue avec la méthode suivante, l'AMDEC qui, elle, entre dans le détail

des modes de défaillance des éléments d'un système. Comme son nom l'indique, l'APR est un préliminaire qui, partant de l'analyse fonctionnelle du système, suppose la défaillance de chaque élément fonctionnel (sans s'occuper du mode de défaillance) et traduit les conséquences de cette défaillance sur le système. L'APR est donc particulièrement indiqué en début de conception afin de ne pas manquer un danger potentiel important.

On trouvera ci-dessous (figure 12) un exemple de tableau d'APR, sans chiffrage de la gravité. C'est l'extrait d'une APR faite sur un tableau Basse Tension comportant un automate qui doit, notamment détecter une surconsommation électrique du tableau.

Pour plus de détails sur l'APR, on pourra consulter le chapitre 6 de l'ouvrage « Sécurité de fonctionnement des systèmes industriels » de A. Villemeur (voir bibliographie).

Fonctions	Equipements considérés	Evénements causant une situation redoutée	Situation redoutée	Evénements causant un accident redouté	Accident redouté	Conséquences redoutées	Remarques
a							
Ouverture du disjoncteur	Dialpact Disjoncteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Non ouverture du disjoncteur	Demande d'ouverture du disjoncteur	Non arrêt du process Non délestage	Surtarification Production du process détériorée	Conséquences dépendantes de l'utilisation du disjoncteur
			Ouverture intempestive du disjoncteur				
Fermeture du disjoncteur	Dialpact Disjoncteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Non fermeture du disjoncteur	Demande de fermeture du disjoncteur	Procédure du process non respectée Relestage impossible	Energie non dispo.	Conséquences dépendantes de l'utilisation du disjoncteur
			Fermeture intempestive du disjoncteur				
b							
Passage de l'information par un Dialpact	Dialpact Capteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Info. erronée du capteur : t° indiquée inf. au seuil	Surconsommation électrique du tableau	Incendie du tableau	Destruction du tableau et arrêt de tous les départs	
Cas direct	Capteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Info. erronée du capteur : t° indiquée inf. au seuil	Surconsommation électrique du tableau	Incendie du tableau	Destruction du tableau et arrêt de tous les départs	
Passage de l'information par un Dialpact	Dialpact Capteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Info. erronée du capteur : t° indiquée sup. au seuil			Demande de délestage inutile	Surconsommation suspectée
Cas direct	Capteur Cartes électroniques Réseau	Un de ces équipements est défaillant	Info. erronée du capteur : t° indiquée sup. au seuil			Demande de délestage inutile	Ici, c'est la mesure de t° qui indique la surconsommation et non celle des courants

Fig. 12 : exemple d'un tableau d'APR pour un tableau BT en configuration « automatique », deux cas sont examinés ici, celui de la commande de disjoncteurs (a) et celui des mesures de température (b).

5.3 La méthode AMDEC

Une AMDEC est une Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité. Un mode de défaillance est un effet par lequel on observe la défaillance d'un élément du système.

Cette définition de la CEI (publication 812) montre que la méthode se base sur la décomposition du système en éléments. Le recueil des données permet de connaître le comportement de chaque élément.

L'architecture matérielle et fonctionnelle du système permet d'induire tous les effets de tous les modes de défaillance de tous les éléments du système.

On inclut dans les AMDEC une évaluation de la criticité de chaque défaillance (cf. **figure 13**). Cette criticité dépend de deux facteurs : la probabilité d'occurrence de la défaillance et la gravité des conséquences.

Une AMDEC permet d'étudier l'influence des défaillances des composants du système. L'intérêt de cette méthode, essentiellement qualitative, est l'exhaustivité. Par contre il faut la compléter pour combiner les effets mis en évidence, c'est l'objet des méthodes décrites dans la suite de ce chapitre 5.

Elément	Fonctions	Modes de défaillance	Causes	Effets	Criticité	Remarques
Disjoncteur	Interrupteur	Refus d'ouverture	Collage	Non délestage	2	
«	«	Refus de fermeture	Mécanique	Non alimentation	2	
«	Protection sur court-circuit	Refus d'ouverture	Collage	Non protection	4	
«	Passage du courant	Ouverture intempestive	Mauvais réglage	Coupage d'alimentation	3	
«	«	Echauffement	Contacts défectueux	Détérioration électronique	2	

Fig. 13 : exemple de tableau AMDEC.

5.4 Les diagrammes de fiabilité

Le diagramme de fiabilité est une façon très simple de représenter un ensemble de composants non réparables. Le calcul de la fiabilité du système ainsi représenté est possible pour les ensembles série-parallèle, en redondance K/N et en pont. Leur application aux systèmes réparables est beaucoup moins systématique.

Les systèmes série-parallèle

Deux éléments sont dits en série si le fonctionnement des deux est nécessaire pour assurer le fonctionnement de l'ensemble. Deux éléments sont dits en parallèle si le fonctionnement d'au moins un des deux est suffisant pour assurer le fonctionnement de l'ensemble (cf. **figure 14**).

Lorsque deux composants sont placés en série l'un ET l'autre doivent fonctionner, il faut donc multiplier leurs fiabilités pour obtenir la fiabilité de l'ensemble :

$$R(t) = R_1(t) \cdot R_2(t).$$

Lorsque deux composants sont placés en parallèle il s'agit cette fois que l'un OU l'autre fonctionne. Il est plus pratique d'utiliser la défiabilité dans ce cas. Pour que le système soit en panne il faut que l'un ET l'autre des deux composants soient en panne, ce qui s'écrit :

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

Les deux formules sont donc :

■ en série :

$$R(t) = R_1(t) \cdot R_2(t)$$



Fig. 14 : les systèmes en série, en parallèle.

■ en parallèle :

$$R(t) = R_1(t) + R_2(t) - R_1(t) \cdot R_2(t)$$

Dans le cas du système parallèle, 1 et 2 sont dits en redondance. Cette redondance est dite passive si l'élément 2 est à l'arrêt tant que l'élément 1 fonctionne. C'est le cas d'un groupe électrogène.

Si 1 et 2 fonctionnent ensemble la redondance est dite active, ce qui est supposé ici. Pour des composants non réparables on calcule la fiabilité de l'ensemble, sachant que les lois suivies par les deux composants sont exponentielles, on a :

■ en série :

$$R(t) = \exp(-\lambda_1 t) \cdot \exp(-\lambda_2 t) = \exp(-(\lambda_1 + \lambda_2)t)$$

R(t) suit une loi exponentielle et :

$$\lambda = \lambda_1 + \lambda_2$$

■ en parallèle :

$$R(t) = \exp(-\lambda_1 t) + \exp(-\lambda_2 t) - \exp(-(\lambda_1 + \lambda_2)t)$$

R(t) ne suit pas une loi exponentielle.

Le taux de défaillance n'est pas constant.

Toutes ces formules se généralisent par associativité à un système de n composants non réparables en série ou en parallèle. On peut combiner ces formules.

Les systèmes à redondance K/N

Un système composé de N éléments est dit à redondance K/N si K éléments suffisent à

assurer sa mission. La redondance est généralement supposée active (cf. figure 15).

Soit $R_i(t)$ la fiabilité du $i^{\text{ème}}$ composant non réparable du système. Dans les cas simples le calcul de la fiabilité de l'ensemble peut se faire par recherche des combinaisons favorables :

■ système 2/3

$$R = R_1 \cdot R_2 + R_1 \cdot R_3 + R_2 \cdot R_3 - 2 R_1 \cdot R_2 \cdot R_3$$

■ système série (N/N) :

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

Lorsque K est petit il est plus facile de calculer $1 - R(t)$, par exemple :

■ système parallèle (1/N) :

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

■ système K/N

Dans le cas où les N éléments sont identiques, pour tout i : $R_i(t) = r(t)$.

On peut alors calculer facilement la fiabilité de l'ensemble par la formule

$$R(t) = \sum_{i=K}^N C_N^i r(t)^i (1-r(t))^{N-i}$$

Les systèmes en pont

On désigne ainsi les systèmes qui ne se réduisent pas à une combinaison série-parallèle. On peut réduire ces systèmes, par itération, au cas ci-dessus (cf. figure 16).

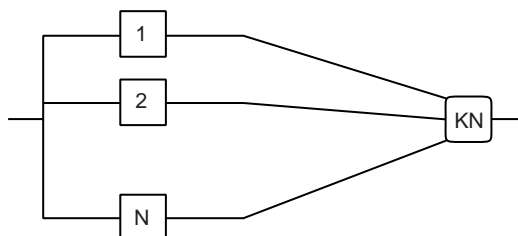


Fig. 15 : les systèmes à redondance K/N.

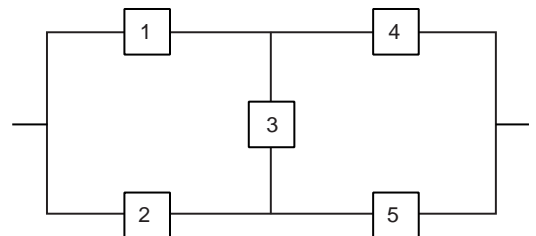


Fig. 16 : système en pont.

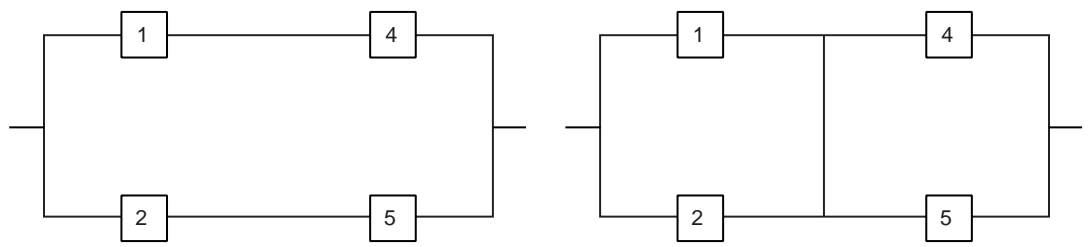


Fig. 17 : décomposition d'un système en pont.

Pour calculer la fiabilité de ce système à partir de celles des cinq composants non réparables il faut utiliser le théorème des probabilités conditionnelles :

$R = R_3 \cdot R$ (sachant que 3 marche)
 $+ (1 - R_3) \cdot R$ (sachant que 3 est défaillant)
 On déduit donc $R(t)$ des résultats de l'étude des deux diagrammes de la figure 17 .

Exemples : fiabilité d'un système de détection d'intrusion.

Le système est constitué de deux capteurs, un capteur de vibration et une cellule photo-électrique, et de deux alarmes, chacune étant reliée à un unique capteur. La fonction du système est d'émettre une alarme en cas d'intrusion activant les capteurs. La durée de mission est fixée à trois mois, c'est la durée maximum d'une absence. On considère chaque élément comme non réparable durant cette période. La maintenance est réalisée avant chaque absence et le système est alors considéré comme neuf. Le système est décrit sur le schéma figure 18 .

Le but est d'évaluer l'amélioration apportée en terme de fiabilité par l'utilisation d'un adaptateur permettant aux deux alarmes de recevoir le signal des deux capteurs. Le système ainsi constitué est représenté sur le schéma figure 19 .

Les données de fiabilité : tous les composants sont non réparables et suivent des lois exponentielles :

- Capteur de vibration : $\lambda_1 = 2 \cdot 10^{-4}$
- Cellule photo-électrique : $\lambda_2 = 10^{-4}$
- Adaptateur : $\lambda_3 = 10^{-5}$
- Alarmes : $\lambda_4 = \lambda_5 = 4 \cdot 10^{-4}$

■ calcul pour le schéma A (figure 18)

On a deux chaînes en parallèle au sens de la fiabilité, chacune comporte deux éléments en série :

- fiabilité chaîne 1 : $R_1(t) \cdot R_4(t)$,
- fiabilité chaîne 2 : $R_2(t) \cdot R_5(t)$; d'où pour le système, $R_A(t) = R_1(t) \cdot R_4(t) + R_2(t) \cdot R_5(t) - R_1(t) \cdot R_4(t) \cdot R_2(t) \cdot R_5(t)$.

En appliquant $R_i(t) = \exp(-\lambda_i \cdot t)$ avec le temps de mission $t = 3 \text{ mois} = 2190 \text{ heures}$, on obtient : $R_A = 0,51$.

■ calcul pour le schéma B (figure 19)

Cette fois on a un schéma en pont. Lorsque l'adaptateur est en panne on a le schéma figure 17. Lorsqu'il fonctionne on a 1 et 2 en parallèle qui sont en série avec 4 et 5 en parallèle. Donc la fiabilité du système avec le schéma figure 17 est :

$$R_B = (1 - R_3) \cdot R + R_3 \cdot (R_1 + R_2 - R_1 \cdot R_2) \cdot (R_4 + R_5 - R_4 \cdot R_5)$$

On obtient cette fois : $R_B = 0,61$.

On constate que l'amélioration est très peu sensible bien que l'adaptateur soit excellent. Sur cet exemple le calcul permet de juger du peu d'intérêt d'un système plus coûteux.

Cas des éléments réparables

On ne peut plus utiliser les diagrammes de fiabilité aussi systématiquement :

- lorsque deux éléments réparables 1 et 2 sont en parallèle, la relation liant $R(t)$ à $R_1(t)$ et $R_2(t)$

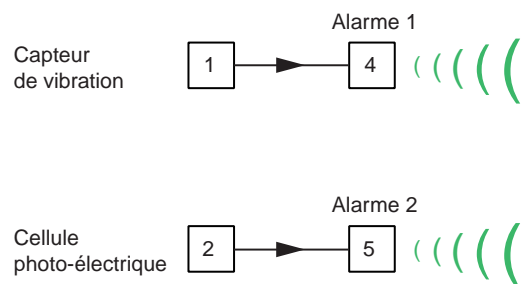


Fig. 18 : alarmes sans couplage : schéma A.

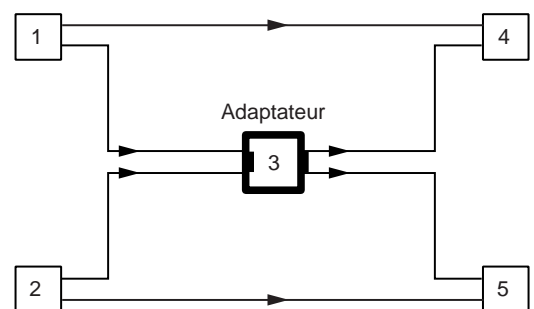


Fig. 19 : chaînes avec couplage : schéma B.

n'est plus vraie. En effet le fonctionnement du système sur $[0,t]$ peut correspondre à un fonctionnement en alternance de 1 et 2. Avec des éléments non réparables un au moins doit fonctionner sur l'ensemble de la période $[0,t]$ alors qu'ici ils peuvent défaillir tous les deux mais pas en même temps.

- Pour deux éléments réparables en série, la relation $R(t) = R_1(t) \cdot R_2(t)$ reste vraie.
- Pour des éléments réparables c'est le chiffrage de la disponibilité qui est le plus souvent demandé. On utilise alors le diagramme de fiabilité, et les mêmes formules que pour le calcul de la fiabilité :

- en série :
 $D(t) = D_1(t) \cdot D_2(t)$,
- en parallèle :
 $D(t) = D_1(t) + D_2(t) - D_1(t) \cdot D_2(t)$.

Ces formules ne sont valables que pour des cas simples.

La relation $D(t) = D_1(t) + D_2(t) - D_1(t) \cdot D_2(t)$ n'est plus vraie si on ne dispose que d'un seul réparateur par exemple. Cet aspect séquentiel, attente de la réparation d'un élément pour réparer l'autre, ne peut pas être modélisé par un simple diagramme. Les graphes d'états (introduits plus loin) sont utilisés dans ce cas.

5.5 Les arbres de défaillance

Ils permettent de calculer la probabilité de « panne » d'un système, et consistent en une représentation graphique des combinaisons d'événements indépendants conduisant à l'apparition d'un événement indésirable ou catastrophique.

A partir de ces arbres, sauf dans les cas simples, c'est par les moyens de l'informatique scientifique et technique que l'on calcule la probabilité d'occurrence ; ensuite on agit éventuellement sur la conception du système pour diminuer la probabilité de défaillance...

Principe de la méthode

La construction de l'arbre se base sur l'analyse du système et sur le choix de l'événement indésirable que l'on désire étudier. La première étape est la recherche des causes immédiates de l'événement sommet, puis des « causes des causes » immédiates et ainsi de suite.

A titre d'exemple, un cas simple : cf. **figure 20** pour le schéma et **figure 21** pour l'arbre de défaillance correspondant.

Une coupe est une combinaison d'événements élémentaires qui conduit à l'événement indésirable.

L'analyse de l'arbre obtenu se décompose en deux phases :

- **l'analyse qualitative** : elle permet d'obtenir les coupes minimales, c'est-à-dire les combinaisons minimales par inclusion qui conduisent à l'événement indésirable. L'ordre d'une coupe est le nombre d'événements élémentaires qui la composent.
- **l'analyse quantitative** : elle est réalisée à partir des coupes minimales et des probabilités d'occurrence des événements de base. On obtient ainsi une approximation de la probabilité d'occurrence de l'événement sommet. Il est nécessaire de s'assurer systématiquement de la validité de l'approximation. Selon les probabilités considérées l'arbre peut être utilisé pour étudier la disponibilité ou la fiabilité.

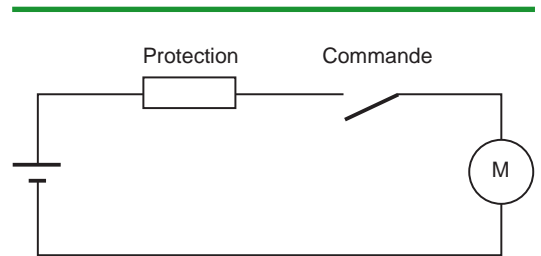


Fig. 20 : chaîne d'alimentation d'un moteur.
L'événement indésirable est : le moteur ne démarre pas.

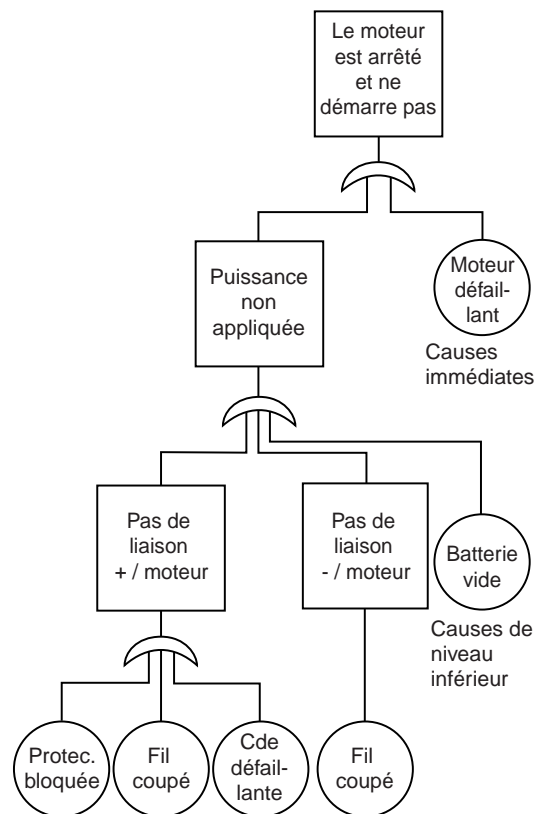


Fig. 21 : arbre de défaillance du circuit de la figure 20.

Deux exemples simples de quantification :

□ un rétroprojecteur avec une lampe en place et une lampe de rechange. L'événement indésirable est : panne de lampe projecteur (cf. **figure 22**).

L'opérateur a deux chances sur mille d'être en panne de lampe.

□ l'alimentation d'une ampoule 220V. L'événement indésirable est : la lampe ne s'allume pas (cf. **figure 23**).

On constate que la probabilité de panne est environ de 0,001. On a une chance sur mille que la lampe ne s'allume pas. L'événement « lampe grillée » est prépondérant.

Il est bien sûr possible d'effectuer un calcul mathématiquement exact de la probabilité d'occurrence. Il se base sur une méthode récursive sans utiliser les « coupes » : on applique les formules de calcul des probabilités pour chaque porte à partir du calcul réalisé pour les sous arbres entrant dans la porte.

L'hypothèse d'indépendance des événements doit être vérifiée mais le calcul est exact. Ce calcul exact permet de valider le calcul approché, mais il est rarement effectué en pratique : en général, les combinaisons autres que les coupes minimales ont des probabilités d'occurrence très faibles car elles sont composées d'un bon nombre d'événements élémentaires ; il est donc souvent inutile et coûteux en temps de calculer ces probabilités.

Application de l'arbre de défaillance avec utilisation des coupes : disponibilité d'un réseau de distribution électrique BT.

La page suivante donne l'arbre de défaillance construit pour étudier la disponibilité sur un départ du réseau dessiné ci-dessous (cf. **figure 24**). On s'intéresse à la disponibilité en énergie électrique en considérant uniquement deux niveaux d'énergie : correct (présence d'énergie), défaillant (absence d'énergie). L'événement sommet indésirable est l'absence d'énergie sur le départ noté E.

La construction de l'arbre (cf. **figure 25**) correspond à certaines hypothèses :

- on a considéré uniquement 2 modes de défaillance pour les disjoncteurs : ouverture intempesive et refus d'ouverture sur court-circuit.

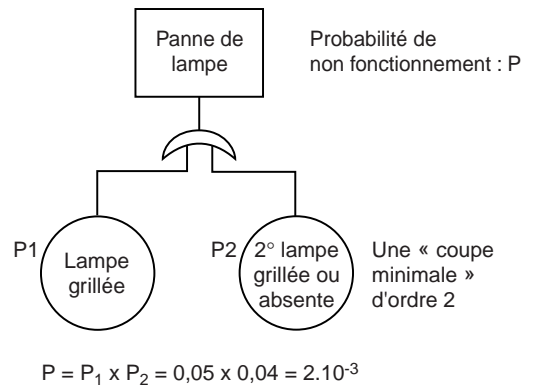


Fig. 22 : arbre de défaillance d'un rétro projecteur.

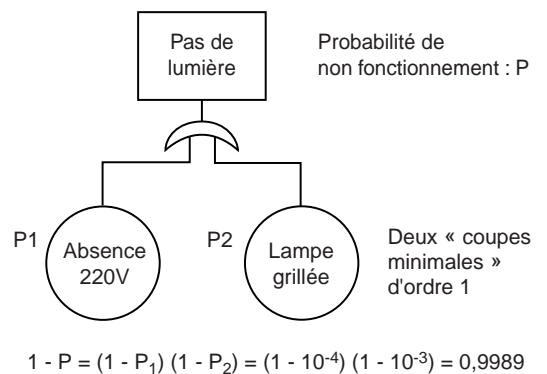


Fig. 23 : arbre de défaillance d'un éclairage.

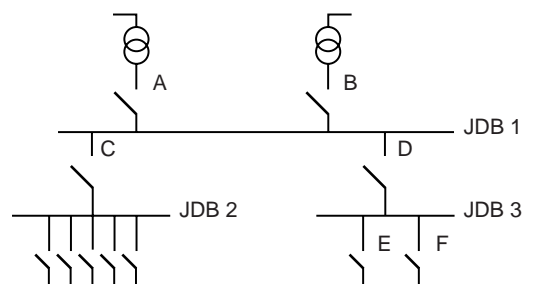


Fig. 24 : réseau de distribution BT.

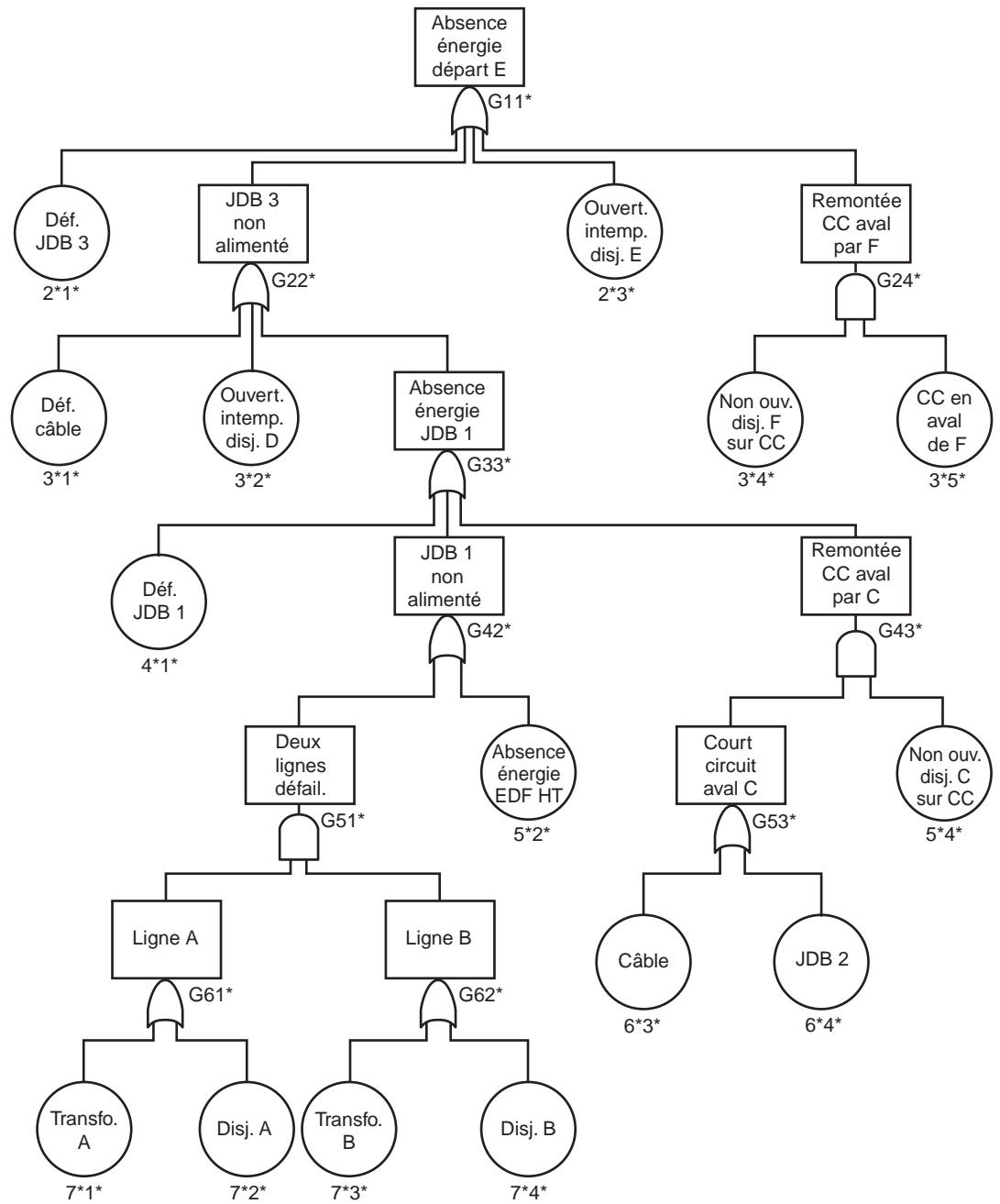


Fig. 25 : arbre de défaillance correspondant au réseau de la figure 24.

■ Chaque voie transformateur peut alimenter seule l'ensemble du réseau prioritaire dont le départ E fait partie.

■ Les deux arrivées EDF sont supposées prises sur deux postes différents.

Ceci réduit le mode de défaillance commun à l'indisponibilité de EDF en haute tension. A chaque événement de l'arbre correspond une probabilité d'occurrence qui est dans ce cas une indisponibilité. Celle des événements élémentaires est calculée par la formule $ID \approx \lambda \cdot MTTR$, avec :

λ : le taux de défaillance de l'élément, pour un mode de défaillance donné, obtenu par recueils des retours d'expérience ;

MTTR : le temps moyen de réparation qui dépend de l'élément et de l'installation (technologie, localisation géographique, contrat...).

Parfois on majore une probabilité quand celle-ci est inconnue. On a pris par exemple 10^{-2} comme majorant de la probabilité d'apparition d'un court-circuit en aval de F.

La **figure 26** donne le résultat obtenu pour l'indisponibilité sur le départ E, soit environ 10^{-5} , ce qui correspond à 5 mn par an. La recherche des coupes minimales permet non seulement d'obtenir la probabilité d'occurrence de l'évènement sommet mais aussi la contribution de chacune des coupes. La même figure 26 donne la liste des coupes minimales et leur contribution exprimée en %. Cette mesure de la contribution est appelée importance.

L'examen des importances relatives montre que le câble reliant le jeu de barres 1 au jeu de barres 3, (3^e coupe minimale), est critique ainsi que, dans une moindre mesure, les deux jeux de barres auxquels il est relié. On constate de plus que l'amélioration de ces éléments rendra la réseau EDF critique. Pour améliorer encore la disponibilité il faudra faire appel à une source de

Indisponibilité : $1,1 \cdot 10^{-3}$

Liste des coupes minimales (indiquées sur l'arbre) et contribution en % :

1	: 2*1*	:	9,5
2	: 2*3*	:	1,6
3	: 3*1*	:	68
4	: 3*2*	:	1,6
5	: 3*4*, 3*5*	:	,013
6	: 4*1*	:	9,5
7	: 5*2*	:	9,9
8	: 5*4*, 6*3*	:	9,1 E - 6
9	: 5*4*, 6*4*	:	3,2 E - 6
10	: 7*1*, 7*3*	:	,00058
11	: 7*1*, 7*4*	:	1,3 E - 5
12	: 7*2*, 7*3*	:	1,3 E - 5
13	: 7*2*, 7*4*	:	2,7 E - 7

Fig. 26 : contribution des éléments du réseau à l'indisponibilité.

secours autonome du type générateur diesel. L'étude de la disponibilité d'une alimentation électrique est détaillée dans le Cahier Technique Schneider Electric n° 184 intitulé « Etude de sûreté des installations électriques ».

Remarque sur les arbres de défaillance

Les systèmes avec reconfiguration et stratégies de maintenance complexes sont difficilement modélisables par un arbre de défaillance. Par exemple, lorsque deux composants sont en redondance, la défaillance du deuxième composant n'a un sens que s'il y a auparavant défaillance du premier composant. Cet aspect temporel de des pannes ne peut pas être pris en compte dans les arbres de défaillances, contrairement aux graphes d'état et réseaux de Pétri présentés ci-après.

5.6 Les graphes d'états

Les graphes d'états (appelés aussi graphes de Markov) permettent une modélisation sous certaines hypothèses. Les étapes successives sont la construction d'un graphe, la résolution des équations de base et l'interprétation des résultats en terme de fiabilité et de disponibilité. La résolution est grandement simplifiée par un calcul limité aux grandeurs indépendantes du temps.

Construction du graphe

Le graphe représente tous les états du système et les transitions possibles entre ces états. Les

transitions entre états correspondent aux événements affectant le fonctionnement des composants du système. Ces événements sont en général des défaillances ou des réparations. Il en résulte que les taux de transition entre états sont essentiellement composés de taux de défaillance ou de réparation (parfois pondérés par des probabilités du type refus de démarrage à la sollicitation).

Le graphe de la **figure 27** représente le comportement d'un système comprenant un unique élément réparable.

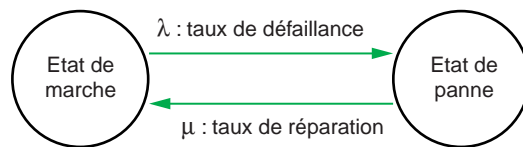


Fig. 27 : graphe d'état élémentaire.

Hypothèses

Un modèle de fonctionnement est dit Markovien si les conditions suivantes sont vérifiées :

- l'évolution du système ne dépend que de l'état qu'il occupe et non du passé,
- les transitions se réalisent suivant des lois exponentielles. Les taux sont constants,
- le nombre d'états est fini,
- deux transitions ne peuvent être simultanées.

Equations

Sous les hypothèses décrites au paragraphe précédent la probabilité d'être dans l'état E_i à l'instant $t + dt$ s'écrit :

$P_i(t+dt) = P_i(t) + \lambda_j P_j(t) dt - \lambda_i P_i(t) dt$ (le système est dans l'état E_i à l'instant t et y reste) + $P_j(t) dt$ (le système vient d'un autre état E_j).

Pour un graphe de n états on obtient n équations différentielles qui donnent l'équation suivante :

$$\frac{d\Pi(t)}{dt} = \Pi(t) \cdot [A]$$

où : $\Pi(t) = [P_1(t), P_2(t), \dots, P_n(t)]$

[A] est appelée matrice de transition du graphe.

La résolution informatique de cette équation sous forme matricielle permet donc d'obtenir la probabilité $P_i(t)$ d'être dans l'état i à l'instant t connaissant les taux de transition du graphe et l'état de départ.

Calcul des différentes grandeurs

La disponibilité est la probabilité de se trouver dans un état de marche on a donc :

$$D(t) = \sum_i P_i(t)$$

P_i = probabilité dans l'état de marche E_i .

La fiabilité est la probabilité d'être dans un état de marche sans jamais être passé par un état de panne.

On construit un graphe où l'on supprime toutes les transitions sortant d'un état de panne vers un état de marche et on obtient des probabilités $P'_i(t)$ et on a alors :

$$R(t) = \sum_i P'_i(t)$$

Il est à noter que deux grandeurs sont obtenues simplement :

- le temps moyen d'occupation d'un état i :

$$T_i = \frac{1}{\sum (\text{Taux sortant de l'état } i)}$$

- la fréquence d'occupation de l'état i :

$$f_i = \frac{P_i}{T_i}$$

Le calcul en temps moyens MTTF, MTTR, MUT, MDT, MTBF se fait par calcul matriciel et en utilisant certaines relations vues au paragraphe 3. Pour le MTTF il faut choisir une distribution initiale des probabilités d'être dans chacun des états.

Applications : onduleurs en parallèle

Un onduleur est un appareil permettant d'améliorer la qualité de l'énergie électrique. Il se place en amont de récepteurs sensibles tels que les ordinateurs et leurs périphériques. On étudie ici un ensemble d'onduleurs en redondance 2/3. L'indisponibilité n'est plus la seule grandeur à considérer : le MTTF permet de connaître le temps moyen avant la première coupure sur l'application. On est amené à construire le graphe d'états. Les trois onduleurs sont identiques ce qui permet de grouper les états correspondant au même nombre d'onduleurs en panne. Les taux de défaillance et de réparation des onduleurs sont notés λ et μ (cf. figure 28).

Le numéro de l'état correspond au nombre d'onduleurs en panne. Chaque onduleur qui fonctionne dans un état E_i ajoute un taux de sortie λ vers l'état E_{i+1} .

Ces taux sont respectivement 3λ , 2λ et λ . En effet, pour passer de l'état 0 à l'état 1 il y a trois possibilités de panne ; pour passer de l'état 1 à l'état 2 il y a deux possibilités de panne, etc.

Les états de marche sont les états 0 et 1. Par hypothèse le nombre de réparateurs est suffisant pour que trois réparations puissent être en cours simultanément. Les taux de transition correspondant aux réparations sont donc proportionnels au nombre d'onduleurs en panne dans l'état considéré. Les données numériques sont les suivantes :

$$\lambda = 2 \cdot 10^{-5} \text{ h}^{-1} ; \mu = 10^{-1} \text{ h}^{-1}$$

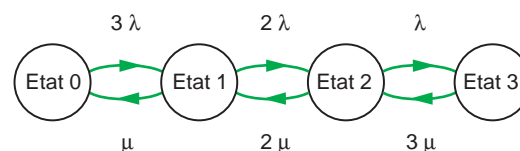


Fig. 28 : onduleurs en parallèle.

Paramètres constants :

Indisponibilité	: 1,199360 E-07	Disponibilité	: 9,999999 E-01
MTTF	: 4,169167 E+07	MTTR	: 8,333667 E+00
MUT	: 4,169167 E+07	MDT	: 5,000333 E+00
MTBF	: 4,169167 E+07		

Fig. 29 : valeurs relatives au schéma de la figure 28.

La figure 29 donne les résultats obtenus lors du calcul des grandeurs indépendantes du temps. On constate que le MTTF vaut $4,17 \cdot 10^7$ heures alors que sans redondance (système 3/3) le MTTF vaut $1/3 \cdot 1,67 \cdot 10^4$ heures.

Pour l'indisponibilité asymptotique on passe de $1,19 \cdot 10^{-7}$ pour le système étudié à $6 \cdot 10^{-4}$ sans redondance (système 3/3). La différence entre

ces deux valeurs se visualise très bien sur le graphe. Dans le cas de la redondance 2/3 l'indisponibilité se calcule en sommant les probabilités des deux états de panne soit : $ID = P_2 + P_3$ alors que sans redondance on somme sur trois états de panne : $ID = P_1 + P_2 + P_3$.

5.7 Les réseaux de Pétri

Un système est représenté par des places, des transitions et des jetons. Le franchissement d'une transition par un jeton correspond à un événement fonctionnel ou dysfonctionnel possible du système. Ces transitions peuvent être associées à n'importe quel type de loi probabiliste, contrairement aux graphes d'états qui supposent des transitions suivant des lois exponentielles. Seule la simulation permet de résoudre de tels calculs.

Le réseau de Pétri de la figure 30 représente les différentes défaillances que le système « distribution électrique » (d'une industrie par exemple) peut subir. Ce système est composé d'une arrivée EDF et de groupes électrogènes qui prennent le relais si EDF est défaillant.

- A la transition n° 1 est associée la probabilité de défaillance de « l'alimentation EDF ».
- A la transition n° 2 est associée les probabilités de démarrage et de non démarrage des groupes électrogènes.
- A la transition n° 3 est associée la probabilité de défaillances en fonctionnement des groupes électrogènes.

La modélisation d'un système par réseau de Pétri est la modélisation la plus proche du fonctionnement réel du système étudié. Par exemple, un temps de réparation constant est un cas de figure courant et peut être modélisé tel quel dans un réseau de Pétri, alors que si l'on modélise par graphes d'état (technique précédente), on est obligé de supposer que ce temps de réparation suit une loi exponentielle.

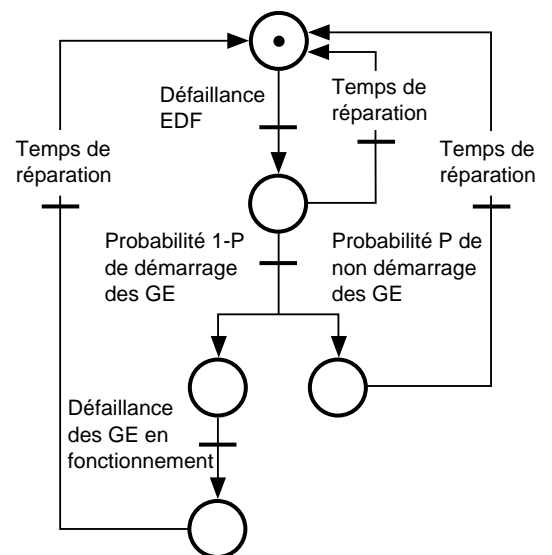


Fig. 30 : modélisation de la distribution électrique par réseau de Pétri.

Mais compte tenu des limites liées à la simulation, cette technique n'est pas utilisée systématiquement : pour être précis, il faut réaliser un grand nombre de simulations et le temps de calcul peut être très long si l'estimation des mesures est liée à des événements rares. Certes, l'augmentation effrénée de la puissance des ordinateurs de bureau tend à gommer cet inconvénient.

5.8 Choix d'une technique de modélisation

On trouvera un tableau détaillé pour faire ce choix dans le Cahier Technique n° 184 « Etudes de sûreté des installations électriques » mais on peut retenir la faiblesse principale de chacune des trois méthodes utilisées (arbres de défaillances, graphes d'état, réseau de Pétri), les diagrammes de fiabilité se cantonnant à des systèmes que l'on rencontre rarement dans la complexité industrielle d'aujourd'hui, à savoir :

- les arbres de défaillance ne peuvent traiter l'aspect temporel des pannes donc les reconfigurations, pourtant fréquentes, en particulier dans la distribution électrique,
- les graphes d'état supposent que les durées de vie et de réparation des composants du système suivent toutes une loi exponentielle,

ce qui est peu réaliste dans certains cas (durée de vie de composants mécaniques soumis à usure, temps de réparation constant...),

- les réseaux de Pétri sont plus compliqués à mettre en œuvre, la traçabilité des erreurs faite lors de la modélisation n'est pas très bonne et les temps de simulation peuvent être très longs lorsque des événements rares sont impliqués.

Etant donné l'amélioration des moyens de calcul, la tendance est à l'utilisation de plus en plus intensive de la simulation par réseau de Pétri, sauf dans le cas de systèmes assez simples où la mise en œuvre des deux autres méthodes est plus rapide pour un résultat équivalent.

6 Maintenance et logistique : de plus en plus complexe...

Dans la conception de la sûreté intervient la maintenance : il est plus tolérable qu'un système tombe fréquemment en panne s'il est réparable instantanément. Ainsi, pour un risque de panne

donné il existe un optimum en terme de maintenance et de stock de pièces de rechange pour garantir un niveau de fiabilité et/ou de disponibilité donné.

6.1 Optimisation de la Maintenance par la Fiabilité (O.M.F.)

Cette méthode apparue dans les années 60 dans le domaine aéronautique, a été reprise par EDF en 1990 pour la maintenance du parc nucléaire et tend à s'appliquer dans bon nombre de sites industriels complexes où des opérations de maintenance sont faites. Cette méthode poursuit trois buts :

- réduire des coûts de maintenance sans dégradation de la fiabilité,
- améliorer la sécurité et la disponibilité des installations (en étant plus pertinent sur les périodicités et les éléments à maintenir),
- maîtriser la durée de vie des équipements (parfois supérieure à la durée de carrière des opérateurs de maintenance).

Elle s'appuie sur deux règles de « bon sens » :
■ classer les défaillances du système par ordre de priorité pour leur assigner une maintenance adaptée : s'il est nécessaire de détecter la défaillance, la maintenance doit être préventive ; s'il suffit de réparer la défaillance, la maintenance peut n'être que corrective,

- utiliser les retours d'expériences sur les défaillances passées pour axer la maintenance sur les composants les moins fiables.

6.2 Soutien Logistique Intégré (S.L.I.)

Cette démarche devient indispensable lorsqu'on doit par exemple assurer la disponibilité de plusieurs systèmes à partir de centres logistiques géographiquement distants : combien de pièces de rechange doit-on prévoir pour l'ensemble des systèmes ? Vaut-il mieux stocker ces pièces de rechange auprès de chacun des systèmes ou les stocker en un seul endroit ?

Le S.L.I. a donc pour objectifs de :

- Maîtriser le rapport « coût global de possession/disponibilité opérationnelle ».
- Prendre en compte des exigences de soutien dès la conception du système (d'où le terme « intégré »).

Cette démarche très globale se traduit en particulier par des optimisations complexes des lots de rechange, optimisations impossibles à faire « à la main », avec une feuille de papier et un crayon. Ces calculs sont effectués à l'aide de programmes informatiques faisant appel à plusieurs domaines des mathématiques appliquées (probabilités, recherche opérationnelle).

Pour plus de détails, on pourra consulter « L'analyse du soutien logistique et son enregistrement » (voir bibliographie).

7 Conclusion

La sûreté, notion de plus en plus importante en terme de confort, d'efficacité, de sécurité, se maîtrise et se calcule. Elle se conçoit à travers les appareils, les architectures, les systèmes. Elle fait de plus en plus partie des cahiers des charges et des clauses contractuelles.

L'existence des méthodes et outils de la sûreté permettent aujourd'hui de rendre systématique les études de sûreté à la conception et lors des actions d'assurance qualité.

L'approche intuitive, les calculs approchés et « exacts » permettent en se combinant de comparer les configurations, de chiffrer le risque pour la meilleure performance, c'est-à-dire celle qui correspond au besoin clairement exprimé.

Enfin, des méthodes d'optimisation permettent d'alléger les coûts de maintenance et de logistique tout en maintenant le niveau de sûreté exigé.

Bibliographie et normes

Normes

- CEI 60191/UTE C20310 : Liste des termes de base, définitions et mathématiques applicables à la fiabilité.
- CEI 362/UTE C20313 : Guide pour l'acquisition des données de fiabilité, de disponibilité et de maintenabilité à partir des résultats d'exploitation des dispositifs électroniques.
- CEI 305/UTE C20321 à 20327 : Essai de fiabilité des équipements.
- CEI 706/X 60310 ET 60312 : Guide maintenabilité de matériel.
- CEI 812/x 60510 : Techniques d'analyse de la fiabilité des systèmes.
Procédure d'Analyse des Modes de Défaillance et de leurs Effets (AMDE).
- CEI 863/x 60520 : Prévion des caractéristiques de fiabilité, maintenabilité et disponibilité.
- CEI 61508 : Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité.

Cahiers techniques Schneider Electric

- Etude de sûreté des installations électriques. S. LOGIACO 1999, Cahier technique n° 184.

Participation de Schneider Electric à différents groupes de travail :

- Groupe statistiques du comité 56 (normes de fiabilité) de la CEI.
- Sûreté du logiciel au groupe Européen EWICS - TC7 : computer and critical applications.

Ouvrages divers

- Military Handbook 217 F (notice 2) Department of Defense (US) - 1995.
- Recueil de données de fiabilité du CNET (Centre National d'Etudes des Télécommunications) - 1999.
- Documents Std 493 et 500 de l'IEEE (Institute of Electrical and Electronics Engineers) 1984 et 1997.
- Document NPRD97 (Nonelectronics Parts Reliability Data du Reliability Analysis Center (Department of Defense US) - 1997.
- « Fiabilité des systèmes »
A. PAGÉS et M. GONDRAN - Eyrolles 1983.
- « Sûreté de fonctionnement des systèmes industriels »
A. VILLEMEUR - Eyrolles 1988.
- Vocabulaire Electrotechnique International VEI 191 - Juin 1988.
- Actes de la 15^e conférence Inter Ram à Portland, Oregon - Juin 1988.
- « Techniques de fiabilité en mécanique »
Cl. MARCOVICI et J. Cl. LIGERON - Pic 1974.
- « L'analyse du soutien logistique et son enregistrement »
M. PREVOST et C. WAROQUIER
Technique et Documentation (Lavoisier 1994).

Schneider Electric

Direction Scientifique et Technique,
Service Communication Technique
F-38050 Grenoble cedex 9
Télécopie : (33) 04 76 57 98 60

Réalisation : AXESS - Saint-Péray (07).
Edition : Schneider Electric
Impression : Imprimerie du Pont de Claix - Claix - 1000.
- 100 FF-