

Chapitre 1

Introduction à la sûreté de Fonctionnement

1. Définition et Evolution de la discipline

Définition de la sûreté de fonctionnement : *La sûreté de fonctionnement (dependability, SdF) consiste à évaluer les risques potentiels, prévoir l'occurrence des défaillances et tenter de minimiser les conséquences des situations catastrophiques lorsqu'elles se présentent.*

La Sûreté de fonctionnement est appelée la science des « défaillances ». D'autres désignations existent suivant les domaines d'applications : analyse de risque (milieu pétrolier), aléatique, cyndinique (science du danger), FMDS (Fiabilité, Maintenabilité, Disponibilité, Sécurité), en anglais RAMS (Reliability, Availability, Maintainability and Safety). Elle se caractérise à la fois par les études structurelles statiques et dynamiques des systèmes, du point de vue prévisionnel mais aussi opérationnel et expérimental (essais, accidents), en tenant compte des aspects probabilités et des conséquences induites par les défaillances techniques et humaines. Cette discipline intervient non seulement au niveau de systèmes déjà construits mais aussi au niveau conceptuel pour la réalisation des systèmes.

Introduite en 1962 pour traduire le terme anglais reliability, la fiabilité est la probabilité de non-défaillance d'un équipement sur un intervalle de temps donné (du latin fidare : faire confiance, fidus : fidèle et du latin médiéval fiabete ce qui est digne de confiance). La disponibilité se définit par la probabilité d'être en état d'accomplir sa fonction à un instant donné. Anglicisme introduit vers 1965, la maintenabilité est l'aptitude d'un système à être maintenu en état. Elle correspond à la probabilité que la remise en état d'une entité en panne soit effectuée dans un intervalle de temps.

Les mots sûreté et sécurité ont en fait la même racine étymologique (latin securus : sûr). Le terme sûreté est plutôt utilisé par les techniciens pour la conception ou l'exploitation de biens et de services pour qualifier la fiabilité et la disponibilité du fonctionnement des installations.

La Sûreté de fonctionnement s'est développée principalement au cours du 20e siècle pour être actuellement un domaine incontournable pour les industries à risques mais aussi, de plus en

plus, pour toute l'industrie, en raison de sa corrélation avec la notion de qualité, les problèmes ergonomiques (relation homme-machine) et l'impact sur l'environnement.

Sûreté de Fonctionnement			
Aptitude à assurer un service spécifié			
Sécurité	Disponibilité		
Aptitude à ne présenter aucun danger pour les personnes, les biens et l'environnement	Aptitude à être en état de marche à un instant donné ou pendant un intervalle de temps donné		
	Fiabilité	Maintenabilité	Logistique de maintenance
	Aptitude à ne pas présenter des défaillances dans une durée déterminée	Aptitude à être remis en service dans une durée donnée	Politique et moyens de maintenance

Tableau 1 : Disciplines de la sûreté de fonctionnement

2. Défaillances, fonctions d'un système et de ses composants

2.1 Définition de la défaillance fonctionnelle

C'est la cessation de l'aptitude d'un dispositif à accomplir une fonction requise.

Une défaillance est « l'altération ou la cessation de l'aptitude d'un ensemble à accomplir sa ou ses fonction(s) requise(s) avec les performances définies dans les spécifications techniques».

L'ensemble est indisponible suite à la défaillance. La cessation de l'aptitude conduit l'entité à être dans un état appelé panne.

Un ensemble est défaillant si ses capacités fonctionnelles sont interrompues (panne ou arrêt volontaire par action d'un système interne de protection ou une procédure manuelle équivalente). Dans le cas d'une dégradation sans perte totale de la fonction, on considère qu'il s'agit d'une défaillance si sa performance tombe au dessous d'un seuil défini, lorsqu'un tel seuil minimal est contenu dans les spécifications fonctionnelles du matériel.

Il s'ensuit qu'un ensemble est défaillant s'il est considéré ou déclaré incapable d'assurer les fonctions requises par l'exploitant utilisant des critères fonctionnels simples. Toute étude de fiabilité implique l'acceptation de deux états totalement exclusifs : le fonctionnement normal et le fonctionnement défaillant. Les passages d'un état de fonctionnement normal à un état défaillant pouvant se manifester en fonction du temps de manière progressive, soudaine ou de façon aléatoire, la fiabilité ne connaît pas la notion de défaillance partielle ou progressive. La figure 1 représente trois cas conduisant tous à une défaillance.

Cette définition inclut de façon très explicite la perte de la fonction d'une entité et, pour cette raison, elle porte souvent à des interprétations différentes suivant les intervenants. Certains

secteurs industriels, pour lever cette ambiguïté, ont dressé des listes standardisées de défaillances fonctionnelles.

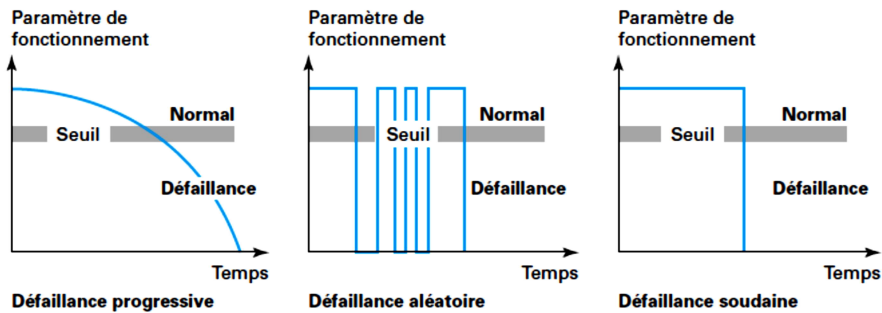


Figure 1 : Cas de figure conduisant tous à la défaillance

Exemple : si l'on considère un moteur électrique dont la fonction principale est de convertir une énergie électrique en énergie mécanique, le refus de démarrage est une défaillance fonctionnelle du moteur. Dans d'autres secteurs industriels, en adoptant une approche matérielle de la défaillance, une perte de l'isolement du stator sera considérée comme une défaillance.

On utilise généralement une échelle de gravité des effets et on considère traditionnellement 4 catégories de défaillances. Ces catégories sont représentées dans le tableau 1.

Défaillance mineure (minor)	Défaillance qui nuit au bon fonctionnement d'un système en causant un dommage négligeable au système ou à son environnement sans présenter de risque pour l'homme
Défaillance significative (major)	Défaillance qui nuit au bon fonctionnement sans causer de dommage notable ni présenter de risque important pour l'homme
Défaillance critique (hazardous)	Défaillance qui entraîne la perte d'une (ou des) fonction(s) essentielle(s) du système et cause des dommages importants au système en ne présentant qu'un risque négligeable de mort ou de blessure.
Défaillance catastrophique (catastrophic)	Défaillance qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) du système en causant des dommages importants au système ou à son environnement et/ou entraîne la mort ou des dommages corporels

Tableau 2 : Classification des défaillances en fonction des effets

La défaillance d'une entité résulte de causes de défaillance ; celles-ci sont définies comme des circonstances liées à la conception, la fabrication ou l'emploi et qui ont entraîné une défaillance. Ces causes sont le résultat d'activation d'erreur suite à des fautes.

Définition Erreur / Defect : La cause de la défaillance est une erreur affectant une partie de l'état du système (par exemple, une variable erronée).

Définition Faute / Fault : La cause de l'erreur est une faute (par exemple un court-circuit sur un composant, une perturbation électromagnétique ou une faute de développement logiciel).

Définition Panne : La panne est l'inaptitude d'une entité à accomplir une mission. Une panne résulte toujours d'une défaillance.

Les relations entre les notions précédentes sont décrites dans la figure 2. Les définitions sont récursives car la défaillance d'un composant est une faute pour le système qui le contient. Ainsi, les défaillances résultent souvent de phénomènes de propagations d'erreur.

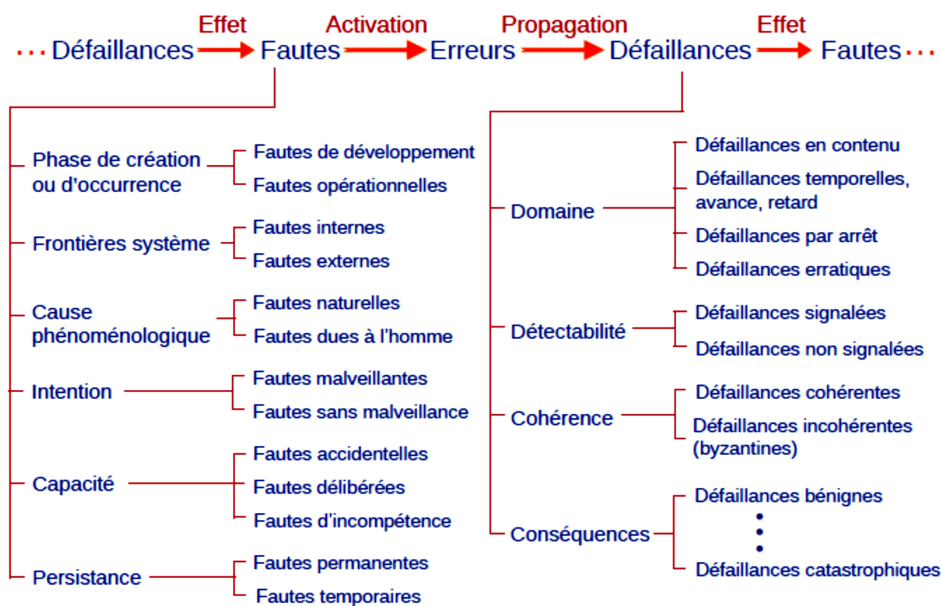


Figure 2 : Enchaînement et propagation des erreurs

Définition Mode de défaillance / Failure mode : Un mode de défaillance est l'effet par lequel une défaillance est observée. Plus, précisément, il s'agit d'un des états possibles d'une entité en panne pour une fonction requise donnée.

Mode de défaillance	Explication
Fonctionnement prématuré (ou intempestif)	Fonctionne alors que ce n'est pas prévu à cet instant
ne fonctionne pas au moment prévu	ne démarre pas lors de la sollicitation
ne s'arrête pas au moment prévu	continue à fonctionner alors que ce n'est pas prévu
défaillance en fonctionnement	

Tableau 3 : Modes de défaillance

2.2 Fonctions

La compréhension de la notion de fonction et de ses paramètres est l'élément clé sur lequel reposent les analyses de Sûreté de fonctionnement car on recherche les éléments matériels qui vont entraîner la perte ou la dégradation des fonctions.

L'AFNOR définit une fonction comme « l'action d'une entité ou de l'un de ses constituants exprimée en termes de finalité ».

Cette définition de nature qualitative est indispensable pour décrire de façon globale une fonction. La fonction fait appel à des notions qualitatives et quantitatives.

Pour un système tel qu'un propulseur à poudre, la description de sa fonction est simple : fournir une poussée nominale de 15 t pendant 30 s. Cette définition donne ses caractéristiques en termes quantitatifs. Un moteur électrique possède une fonction de base consistant à convertir de l'énergie mécanique en énergie électrique.

Les différences entre ces fonctions sont quelquefois subtiles et l'acceptation de leur terminologie doit toujours faire l'objet d'une acceptation au sens d'une même entreprise et de ses prestataires. Pour des systèmes plus complexes, il est indispensable de classer et de hiérarchiser la nature des fonctions :

- principales ;
- secondaires ;
- de protection ;
- redondantes.

- Fonctions principales

Une fonction principale peut se définir comme étant la raison d'être d'un bien ou d'un système défini souvent avec ses caractéristiques associées (durée, caractéristiques physiques, chimiques...).

Par exemple, une première définition générale de la fonction principale d'une chaudière est de fournir de la vapeur.

- Fonctions secondaires

Dans de nombreux cas, un système assure d'autres fonctions que la fonction principale. Ces fonctions sont appelées fonctions secondaires et leur perte peut également avoir des conséquences catastrophiques.

En reprenant l'exemple de la chaudière, une fonction secondaire est de maintenir l'intégrité du confinement de la vapeur. L'existence d'une fuite ou le risque d'une explosion entraînerait une défaillance de la fonction principale. Le calorifugeage de la chaudière est une autre fonction secondaire de la chaudière ayant pour but de minimiser les pertes thermiques.

- Fonctions de protection

Les fonctions de protection ont pour but de garantir, par des moyens de signalisation ou la mise en route de systèmes redondants, la sécurité des biens, des personnes et de l'environnement. Ces fonctions de protection sont assurées par des systèmes de signalisation, d'alarme ou de protection automatique.

Dans le cas d'une chaudière à vapeur alimentée par un brûleur à gaz, les soupapes de sécurité assurent une protection passive contre le risque de surpression, le système de mesure de pression et de température permet aux opérateurs de contrôler les anomalies de fonctionnement et le système de détection de gaz à l'intérieur de la chaudière a pour rôle d'éviter son explosion.

- Fonctions redondantes

Dans les industries telles que celles des secteurs aéronautiques, nucléaires et spatiaux, des systèmes ou des matériels redondants (doublés, triplés ou quadruplés) sont couramment mis en œuvre pour assurer le niveau requis de sécurité ou de sûreté. Ces systèmes redondants peuvent fonctionner en permanence (redondance active) ou être en attente (redondance passive).

Dans l'industrie automobile, c'est ainsi que l'on équipe certains véhicules avec un double circuit de freinage. Pour un avion bimoteur, les deux moteurs illustrent la redondance active. En effet, en cas de panne d'un des moteurs, le propulseur restant a été conçu pour pouvoir ramener l'aéronef sur un terrain d'atterrissage avec toutes les conditions de sécurité.

3. Description des procédés industriels

La notion de processus industriel recouvre des secteurs industriels très variés. Au sens très large, un processus assure la fabrication d'un produit ou fournit un service. Ainsi une raffinerie a pour objectif de fournir des produits pétroliers élaborés ; une centrale électrique a pour vocation de produire du courant électrique ; un avion assure un service de transport de biens ou de personnes. Un ordinateur s'assimile également à un processus puisqu'il fournit un service de calculs scientifiques ou de gestion.

Ces quelques exemples illustrent la notion très large de processus industriels. Conceptuellement, on appellera processus industriel, une installation complexe assumant un objectif fonctionnel de haut niveau (production de biens ou de services).

Pour assurer ces objectifs fonctionnels de haut niveau, le processus fait appel à un ensemble de systèmes interconnectés ou en interaction. Chaque système assure une ou plusieurs fonctions bien définie(s). Les systèmes peuvent être décomposés en sous-systèmes assumant à leur tour généralement un seul objectif fonctionnel. L'étape suivante concerne la décomposition des systèmes ou sous-systèmes en composants ou matériels bien déterminés.

Selon les spécificités des secteurs industriels concernés, les méthodes de description des éléments constitutifs d'un procédé industriel font appel à des découpages matériels ou fonctionnels. Dans le cas d'une description matérielle, on ne prend en compte que la morphologie physique des matériels par un descriptif mettant en œuvre la notion, par exemple, de matériels, composants, pièces élémentaires. Dans le cas d'une description

fonctionnelle, on s'attache à décrire le procédé à l'aide d'entités fonctionnelles telles que groupements fonctionnels, ensembles fonctionnels, sous-ensembles fonctionnels... La lecture attentive des normes concernant la qualité, la maintenance, la maintenabilité, la maintenance intégrée à la conception, le soutien logistique intégrée (SLI), la maintenance productive totale (TPM) font appel à une telle variété de termes qu'il est souvent difficile de dialoguer même entre spécialistes. En effet, suivant les cultures de maintenance rencontrées dans les différents pays industrialisés (Europe, États-Unis, Canada, Japon, Corée, Russie...) les termes utilisés possèdent un sens et un contenu différents.

Les méthodes fonctionnelles utilisent des formalismes ou des arborescences basées sur des fonctions principales, secondaires, externes et redondantes permettant de comprendre le fonctionnement sans se préoccuper des réalisations matérielles. Ce sont ces méthodes qui sont à l'heure actuelle appliquées par les concepteurs et les équipes chargées des études de Sécurité de fonctionnement.

3.1 Description générale

Les termes suivants s'emploient pour décrire les entités constitutives d'un processus ou d'une installation industrielle sans vouloir leur affecter un sens matériel ou fonctionnel.

- Bien durable

Tout élément, composant, équipement, sous-système, système, matériel de processus, etc., que l'on peut considérer individuellement et qui a pour objectif d'assurer une fonction donnée pendant un temps relativement long, compte tenu de la qualité des opérations de maintenance. Un bien durable peut être relativement simple (machine à laver) ou complexe (avion, centrale nucléaire, ouvrage d'art, etc.).

- Élément

Partie constitutive d'un ensemble ou sous-ensemble quelles qu'en soient la nature ou la dimension.

Exemple : tuyère d'un propulseur.

- Sous-ensemble

Groupement d'éléments associés en fonctionnement entrant dans la constitution d'un ensemble. Le sous-ensemble peut avoir une signification matérielle et/ou fonctionnelle.

Exemple : propulseur d'une fusée.

- Ensemble

Groupement de sous-ensembles assurant une ou plusieurs fonctions techniques qui le rendent apte à remplir une fonction opérationnelle. L'ensemble peut avoir également une signification matérielle et/ou fonctionnelle.

Exemple : les propulseurs d'une fusée permettent le lancement en orbite d'un satellite (fonction opérationnelle) ; les fonctions techniques consistent à réaliser la poussée nécessaire.

3.2 Description fonctionnelle

Une description fonctionnelle se présente généralement sous la forme d'une arborescence hiérarchisée à plusieurs niveaux représentée, sur la figure 3 pour une machine à laver la vaisselle. Dans cet exemple, on n'a représenté que trois niveaux sachant qu'il est possible d'ajouter des niveaux supplémentaires. Cette décomposition fonctionnelle sous forme d'arbre fonctionnel n'est pas la seule méthode disponible. Des méthodes issues des techniques de l'analyse de la valeur et de l'analyse fonctionnelle sont utilisables pour décrire les phases de conception et l'exploitation d'un système industriel (méthodes FAST, RELIASEP®, APTE®, SADT®...). En théorie, cette description fonctionnelle devrait faire abstraction de toute réalisation matérielle. Dans la pratique, surtout pour la description d'installations complexes opérationnelles, on associe très souvent les éléments matériels qui contribuent à réaliser ces fonctions. Trois termes principaux sont largement utilisés pour décrire fonctionnellement une installation industrielle complexe : les systèmes, les sous-systèmes et les composants.

- Système

C'est l'association de sous-systèmes constituant un tout organique complexe, destiné à remplir une fonction générale d'un bien durable complexe.

Exemple : le système de propulsion d'un avion quadriréacteur comporte les 4 réacteurs et sa fonction est de propulser l'avion.

- Sous-système

Le sous-système représente une association de composants destinée à remplir une ou plusieurs fonctions opérationnelles.

Exemple : un réacteur d'un quadriréacteur remplit une partie de la fonction de propulsion durant le décollage et pendant le vol. Il assure par inversion de poussée la fonction de freinage à l'atterrissage.

- Composants

Le composant représente un élément matériel ou un ensemble matériel remplissant une fonction particulière dans un système ou sous-système.

Exemple : le compresseur d'un réacteur d'avion est un composant qui comprime l'air avant son injection dans les chambres de combustion.

Si l'installation industrielle est complexe il est possible de compléter la description par des niveaux inférieurs tels que sous-sous-systèmes, etc.

3.3 Description matérielle

Une description matérielle d'un processus ou d'un équipement fournit essentiellement tous ses éléments constitutifs sans se préoccuper de leurs fonctions. On peut considérer cette décomposition comme une mise à plat des éléments que l'on obtiendrait en effectuant un démontage complet. Elle correspond à une logique de démontage / remontage. De ce fait, elle donne une représentation externe et physique.

La figure 4 représente la décomposition matérielle de la machine à laver la vaisselle. Dans l'industrie, cette méthode de décomposition est particulièrement utile pour établir une

nomenclature des différents éléments pour la gestion des stocks, la mise en oeuvre d'un outil de gestion de maintenance assistée par ordinateur (GMAO) et, dans certains cas, pour servir de support aux banques de données de retour d'expérience. Cette décomposition matérielle comprend des descripteurs matériels tels que pièces, organes, mécanismes, dispositifs, matériels et installations qui vont du plus petit élément (pièce) au plus important (installation).

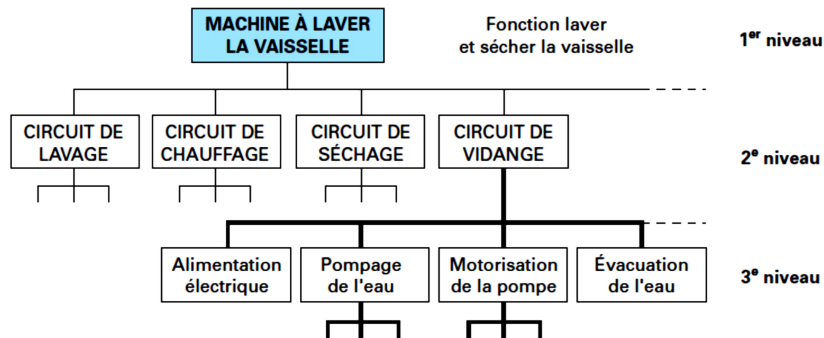


Figure 3 : Décomposition fonctionnelle d'une machine à laver vaisselle

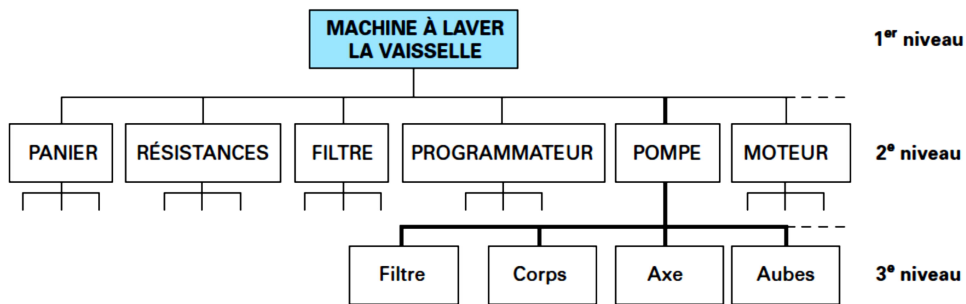


Figure 4 : Décomposition matérielle d'une machine à laver vaisselle

Chapitre 2 :

Concepts de base de la Sûreté de Fonctionnement

1. Rappels sur les probabilités

Les définitions et les méthodes utilisées dans la discipline de la Sûreté de fonctionnement font appel aux théories des probabilités qui vont faire l'objet des principaux rappels en s'appuyant sur une notion concrète en Sûreté de fonctionnement : l'instant d'apparition d'une défaillance.

Considérons une entité dont le fonctionnement au cours du temps sera représenté par la variable $X(t)$. L'état normal de fonctionnement sera représenté par $X(t) = 1$ et un état défaillant sera noté par $X(t) = 0$.

L'instant T d'occurrence d'une défaillance (sauf action délibérée et programmée dans le temps) n'est jamais prévisible et correspond à un événement aléatoire. L'observation du temps d'apparition de la défaillance correspond à une réalisation particulière d'une variable aléatoire dont il conviendra de connaître les caractéristiques en termes de probabilités (figure 5).

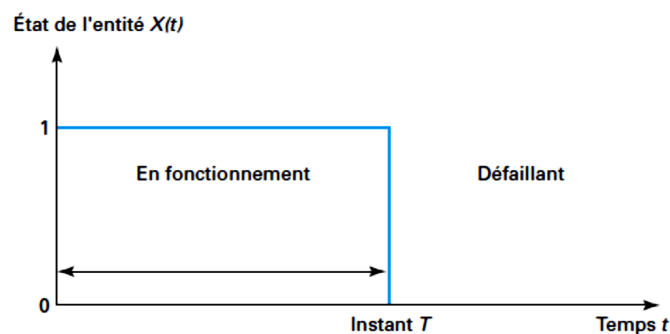


Figure 5 : Représentation de l'état de fonctionnement d'une entité

Notion de variable aléatoire

Une variable aléatoire est une variable réelle dont la valeur est liée au résultat d'une expérience. Ainsi, dans le jeu de jet d'un seul dé, le résultat est une variable aléatoire X pour laquelle nous lisons sur la face du dé les valeurs entières 1, 2, 3, 4, 5 et 6. Plus généralement,

il est possible d'associer à une variable aléatoire un nombre fini ou infini de nombres entiers, réels ou complexes, que l'on notera X.

En Sûreté de fonctionnement, les variables aléatoires discrètes se rencontrent lorsque les événements se produisant sur un intervalle de temps donné sont des nombres entiers. C'est, par exemple, le nombre de cartes électroniques défaillantes par mois dans un système de contrôle-commande. Les variables aléatoires continues rencontrées en Sûreté de fonctionnement peuvent prendre toutes les valeurs réelles entre 0 et l'infini. Ainsi, l'instant d'apparition d'une défaillance d'une structure métallique entre dans cette catégorie.

Notion de probabilité d'un événement

En utilisant une approche issue de la théorie de la mesure, la probabilité d'un événement peut se définir comme étant la limite d'une fréquence relative observée de cet élément lorsque le nombre d'essais ou d'observations tend vers l'infini.

Considérons une expérience dont les événements discrets possibles sont A, B et C et que l'on répète N fois.

Soit N_A , N_B et N_C , le nombre de fois où les événements A, B et C ont été observés avec :

$$N_A + N_B + N_C = N.$$

La probabilité $P(A)$ de l'événement A est définie par :

$$P(A) = \lim_{x \rightarrow \infty} \frac{N_A}{N}$$

La probabilité d'un événement est un nombre réel toujours compris entre 0 et 1 :

$$0 \leq P(A) \leq 1$$

Ainsi, dans le jeu de jet d'un seul dé, la probabilité d'obtenir 1, 2, 3, 4, 5 ou 6 est égale à 1/6.

Axiomes des probabilités

En notant, par convention, les opérateurs logique ET et OU respectivement par \times et $+$, l'axiome des probabilités totales (ou théorème de Poincaré) se formule par :

$$P(A + B) = P(A) + P(B) - P(A.B)$$

Deux événements A et B sont dits incompatibles ou disjoints si $(A.B) = \emptyset$

L'événement consistant à obtenir simultanément A et B est impossible : $P(A.B) = \emptyset$

d'où $P(A + B) = P(A) + P(B)$.

Deux événements sont indépendants si la probabilité d'occurrence de l'événement A ne dépend pas de l'occurrence de l'événement B. Dans ce cas $P(A.B) = P(A).P(B)$.

Probabilités composées ou relation de Bayes

Soient deux événements A et B non disjoints, On appelle probabilité de A conditionnellement à B ou (sachant B) notée $P(A/B)$, la probabilité de réalisation de A sachant que B s'est déjà réalisé.

On définit de même la probabilité de B conditionnellement à A ou (sachant A) notée $P(B/A)$, la probabilité de réalisation de B sachant que A s'est déjà réalisé.

$$P(A \cap B) = P(A)P(B/A) = P(B)P(A/B)$$

$P(A)$ et $P(B)$ sont appelées les probabilités à priori de A et B.

Si les événements A et B sont totalement indépendants, c'est-à-dire si la probabilité d'occurrence de A n'est pas influencée par l'occurrence de B alors :

$$P(A/B) = P(A) \text{ et } P(B/A) = P(B)$$

d'où $P(A \cap B) = P(A) \cdot P(B)$.

Fonction de répartition d'une variable aléatoire continue

La fonction de répartition $F(x)$ d'une variable aléatoire X définie sur $]-\infty, +\infty[$ correspond à la probabilité d'obtenir un résultat inférieur ou égal à une valeur x donnée :

$$F(x) = P(X \leq x)$$

La probabilité d'obtenir un résultat compris entre a et b ($b > a$) est donnée par :

$$P(a \leq X < b) = F(b) - F(a)$$

La densité de probabilité $f(x)$ se déduit de la fonction de répartition $F(x)$ par la relation :

$$f(x) = \frac{dF(x)}{dx}$$

On démontre également que : $P(a \leq x < b) = \int_a^b f(x) dx$

Valeur moyenne et variance d'une variable aléatoire continue

La valeur moyenne m (ou l'espérance mathématique $E(x)$) et la variance $\text{Var}(x)$ d'une variable aléatoire se déduisent de la loi de densité de probabilité $f(x)$ par le calcul des intégrales suivantes :

$$m = \int_{-\infty}^{+\infty} x f(x) dx$$

$$Var(x) = \int_{-\infty}^{+\infty} (x-m)^2 f(x) dx$$

$\sqrt{Var(x)}$ est l'écart type

Ces caractéristiques statistiques sont fondamentales en Sûreté de fonctionnement car elles permettront le calcul du temps moyen de fonctionnement entre défaillance du temps moyen avant remise en service (MTBF, MTTR).

2. Lois de probabilité rencontrées dans les études de fiabilité

Les principales lois utilisées dans les études de Sûreté de fonctionnement sont les suivantes :

Loi exponentielle : utilisée fréquemment car les calculs sont simples.

La densité de probabilité est : $f(t) = \lambda e^{-\lambda t}$ où λ est une constante

La fonction de répartition est : $F(t) = \int_{-\infty}^t f(t) dt = 1 - e^{-\lambda t}$

La moyenne est de $\frac{1}{\lambda}$ et la variance de $\frac{1}{\lambda^2}$.

Cette loi s'applique pour la durée de vie utile représentée dans la courbe en baignoire.

Loi normale : La loi normale ou de Gauss a deux paramètres $N(m, \sigma)$ avec m la moyenne et σ l'écart type.

La densité de probabilité est : $f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-m)^2}{2\sigma^2}}$

La fonction de répartition est : $F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^t e^{-\frac{(t-m)^2}{2\sigma^2}} dx$

Cette loi s'applique à de nombreux phénomènes (incertitude sur des mesures ou des fabrications par exemple).

Loi log-normale : Une variable aléatoire est distribuée suivant une loi log-normale si son logarithme est distribué selon une loi normale.

La densité de probabilité est :

$$f(t) = \frac{1}{\sigma t \sqrt{2\pi}} e^{-\frac{(\ln(t)-\mu)^2}{2\sigma^2}}$$

La fonction de répartition est :

$$F(t) = \frac{1}{\sigma \sqrt{2\pi}} \int_{-\infty}^t \frac{1}{x} e^{-\frac{(\ln(x)-\mu)^2}{2\sigma^2}} dx$$

Avec : μ moyenne des $\ln(t)$,
 σ écart-type des $\ln(t)$.

La moyenne est

$$m = \exp\left(\mu + \frac{\sigma^2}{2}\right)$$

La variance

$$Var(t) = e^{2\mu + \sigma^2} (e^{\sigma^2} - 1).$$

Cette loi est souvent utilisée pour représenter les durées de réparation des composants ou les incertitudes dans la connaissance d'une donnée de sûreté de fonctionnement.

Loi de Weibull : cette loi dépend de 3 paramètres et permet de représenter un grand nombre de distributions expérimentales.

La densité de probabilité est :

$$f(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^\beta} e^{-\frac{(t-\gamma)^\beta}{\eta}}$$

Avec : $\beta > 0$ paramètre de forme (sans unité),
 $\eta > 0$ paramètre d'échelle (en unités de temps), et
 $t > \gamma$ paramètre de position (en unité de temps).

La fonction de répartition est :

$$F(t) = 1 - e^{-\left(\frac{t-\gamma}{\eta}\right)^\beta}$$

La moyenne est :

$$m = \gamma + \eta \Gamma\left(\frac{1+\beta}{\beta}\right)$$

La variance est :

$$Var(t) = \eta^2 \left(\Gamma\left(\frac{2}{\beta} + 1\right) - \Gamma^2\left(\frac{1}{\beta} + 1\right) \right)$$

avec $\Gamma(b) = \int_0^{+\infty} x^{b-1} e^{-x} dx$

3. Concepts de base la sûreté de fonctionnement

Les attributs de la sûreté de fonctionnement sont parfois appelés FDMS pour Fiabilité, Disponibilité, Maintenabilité et Sécurité (RAMSS pour Reliability, Availability, Maintainability, Safety, Security). La fiabilité est la continuité du service, la disponibilité est le fait d'être prêt à l'utilisation, la maintenabilité est l'aptitude à être réparé et la sécurité est l'aptitude à ne pas provoquer d'accidents catastrophiques.

3.1 Fiabilité (Reliability)

La norme NF X 60-500 définit la fiabilité comme « *l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné* ».

L'entité (E) désigne au sens large un composant, sous-système ou système, et la fonction requise est la ou les fonctions que doit accomplir le dispositif pour pleinement remplir la tâche qui lui est assignée.

Considérons l'instant T d'occurrence de la défaillance ; cette variable aléatoire permet de définir la notion de fiabilité qui s'interprète comme la probabilité que l'entité considérée ne tombe pas en panne avant un instant t donné ou bien comme la probabilité qu'elle tombe en panne après l'instant t.

Par extension, on appelle également fiabilité la probabilité associée $R(t)$ à cette notion alors qu'elle n'en est qu'une mesure.

Elle est définie par :

$R(t) = P(E \text{ non défaillante sur la durée } [0, t], \text{ en supposant qu'elle n'est pas défaillante à l'instant } t = 0).$

L'aptitude contraire est appelée défiabilité, et est définie par :

$$\bar{R}(t) = 1 - R(t) = F(t)$$

Si $R(t)$ est la probabilité de ne rencontrer aucune défaillance dans l'intervalle $[0, t]$ sachant que l'entité est non défaillante à $t = 0$, le terme $1 - R(t)$ représente la probabilité que la défaillance se produise entre $[0, t]$.

La fonction $F(t) = 1 - R(t)$ représente la *fonction de répartition* de la variable aléatoire T (instant de la défaillance).

On distingue plusieurs types de fiabilité (termes spécifiques) :

— **la fiabilité opérationnelle** (observée ou estimée) déduite de l'analyse d'entités identiques dans les mêmes conditions opérationnelles à partir de l'exploitation d'un retour d'expérience ;

— **la fiabilité prévisionnelle** (prédite) correspondant à la fiabilité future d'un système et établie par son analyse, connaissant les fiabilités de ses composants ;

— **la fiabilité extrapolée** déduite de la fiabilité opérationnelle par extrapolation ou interpolation pour des conditions ou des durées différentes ;

— **la fiabilité intrinsèque** ou inhérente qui découle directement des paramètres de conception. Sans modification de conception des entités, il n'est pas possible d'obtenir un niveau de fiabilité au plus égal à la fiabilité intrinsèque.

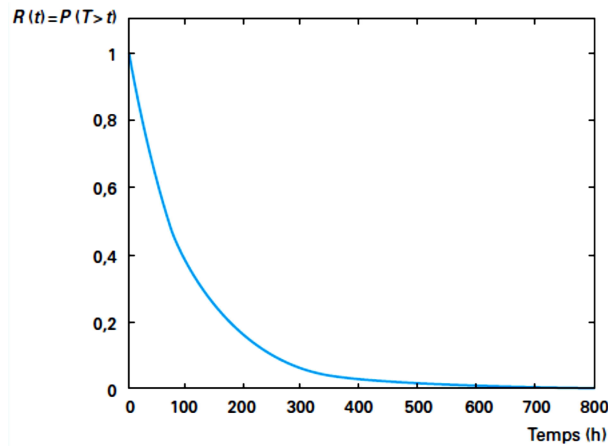


Figure 6 : R(t) pour la loi exponentielle

La connaissance des lois de fiabilité des différentes entités constituant les systèmes industriels est indispensable pour mettre en oeuvre une démarche de Sûreté de fonctionnement.

a. Densité de défaillance

La densité de probabilité de l'instant de la défaillance T s'obtient en dérivant la fonction de répartition F (t) :

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$

Ce terme est appelé la densité de défaillance.

b. Taux de défaillance

A partir de la connaissance des termes R (t), f (t) et F (t), on peut définir la notion de taux de défaillance au temps t qui est noté universellement par $\lambda(t)$. Formellement $\lambda(t) dt$ représente la probabilité d'avoir une défaillance entre (t, t + dt), sachant qu'il n'y a pas eu de défaillance entre sur [0, t]. En appliquant le théorème des probabilités conditionnelles, il vient, si dt est petit :

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

d'où :

$$R(t) = e^{-\int_0^t \lambda(x) dx}$$

Loi	Exponentielle	Weibull
$f(t)$	$\lambda e^{-\lambda t}$	$\frac{\beta(t-\gamma)^{\beta-1}}{\eta^\beta} e^{-\frac{(t-\gamma)^\beta}{\eta}}$
$\lambda(t)$	λ	$\frac{\beta}{\eta} \frac{(t-\gamma)^{\beta-1}}{\eta}$

Tableau 4 : Taux de défaillance pour la loi exponentielle et la loi de Weibull

Pour la loi exponentielle,

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

Courbe caractéristique du taux de défaillance :

- **la période de jeunesse** : quand un système est neuf, on observe souvent des défaillances précoces, dues à des défauts intrinsèques ou des fautes de conception. Le risque de défaillance est donc assez fort au tout début de la vie du système. Ensuite il diminue car, s'il y a des défauts initiaux, ils vont se manifester tôt. λ est donc d'abord décroissant. C'est le rodage pour les matériels mécaniques et le déverminage pour les matériels électroniques ;
- **la vie utile** : pendant cette période, le taux de défaillance est constant et les défaillances sont purement accidentelles ;
- **le vieillissement** : λ se remet à croître car le risque de défaillance va finir par augmenter à cause de l'usure du système.

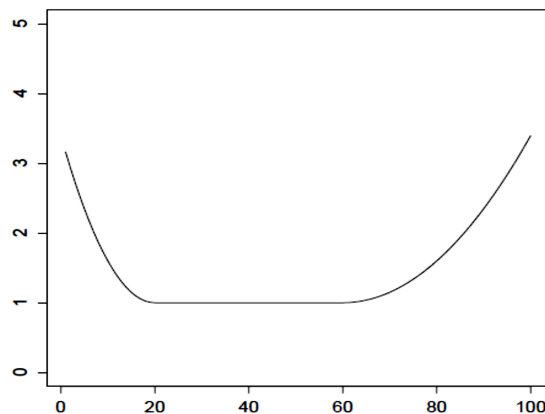


Figure 7 : Taux de défaillance $\lambda(t)$ en forme de baignoire

c. Moyenne de temps de vie avant la première défaillance (MTTF)

Une grandeur moyenne associée à la fiabilité souvent utilisée est le temps moyen de fonctionnement d'une entité ou moyenne de temps de vie avant la première défaillance (Mean operating Time To Failure) :

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

L'utilisation correcte du MTTF dans les calculs de fiabilité d'une entité impose obligatoirement que l'on définisse l'état initial sous peine de grossières erreurs.

En appliquant la loi exponentielle, on obtient :

$$MTTF = \int_0^{+\infty} e^{-\lambda t} dt = \frac{1}{\lambda}$$

On peut également l'obtenir de manière expérimentale puisque :

$$MTTF = \lim_{n \rightarrow \infty} \sum \frac{t_i}{n}$$

3.2 Disponibilité (Availability)

La norme AFNOR X 60-500 définit la disponibilité comme « l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires de maintenance soit assurée ».

La probabilité associée $A(t)$ à l'instant t est aussi appelée disponibilité et s'exprime par :

$$A(t) = P(E \text{ non défaillante à l'instant } t)$$

L'aptitude contraire est appelée indisponibilité et est définie par :

$$\bar{A} = 1 - A(t)$$

La disponibilité $A(t)$ est une grandeur instantanée. L'entité peut donc avoir subi une panne puis une réparation avant l'instant t , contrairement à la fiabilité $R(t)$ qui est une grandeur mesurée sur une durée (intervalle $[0, t]$). La confusion entre disponibilité et fiabilité est due au fait que ces deux concepts sont équivalents quand le système est non réparable. $A(t)$ est donnée aussi par :

$$A(t) = \frac{\mu}{\lambda + \mu} - \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t}$$

L'interprétation physique est illustrée sur la figure (*Disponibilité en fonction du temps t*) où sont représentés les cas d'entités disponibles et non disponibles à l'instant $t = 0$.

Dans l'industrie cela revient au constat que, sous réserve d'une politique de maintenance efficace, au bout d'un temps donné les entités ont atteint leur limite asymptotique de disponibilité.

Comme la fiabilité, plusieurs types de disponibilités peuvent être utilisés :

— **la disponibilité instantanée prévisionnelle** (définie précédemment);

— **la disponibilité moyenne** : moyenne sur un intervalle de temps donné $[t_1, t_2]$ de la disponibilité instantanée prévisionnelle, ou mesurée en phase opérationnelle par la durée de fonctionnement effectif divisée par la durée donnée.

Les grandeurs moyennes associées à la disponibilité les plus courantes sont :

— **Le temps moyen de disponibilité (TMD)** ou durée de bon fonctionnement après réparation, ou Mean Up Time (MUT) : durée moyenne de fonctionnement après la réparation et la défaillance suivante ;

— **Le temps moyen d'indisponibilité (TMI)** ou durée moyenne d'indisponibilité, ou Mean Down Time (MDT) : durée moyenne entre une défaillance et la remise en état suivante ;

— **La durée moyenne entre défaillance notée MTBF** (mean time between failure) : durée moyenne entre deux défaillances consécutives de l'entité. En général, on a la relation :

$$MTBF = MUT + MDT$$

$$MTBF = \frac{\text{Temps de bon fonctionnement}}{\text{nombre de périodes de bon fonctionnement}}$$

$$\lambda = \frac{1}{MTBF}$$

La figure 9 fournit les représentations graphiques de ces définitions en fonction du temps.

La disponibilité asymptotique se déduit du MUT et du MTBF par la relation :

$$A_{\infty} = \frac{MUT}{MTBF}$$

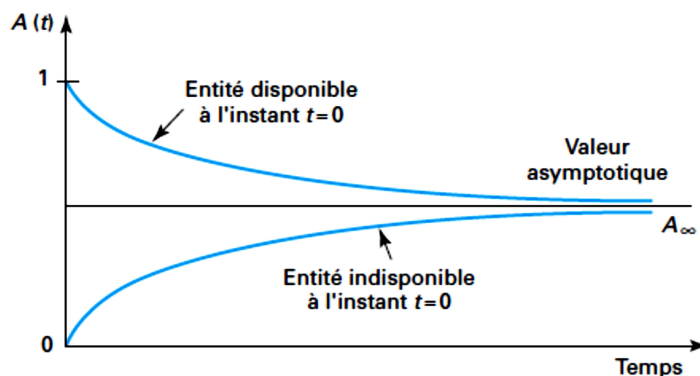


Figure 8 : Disponibilité en fonction du temps t

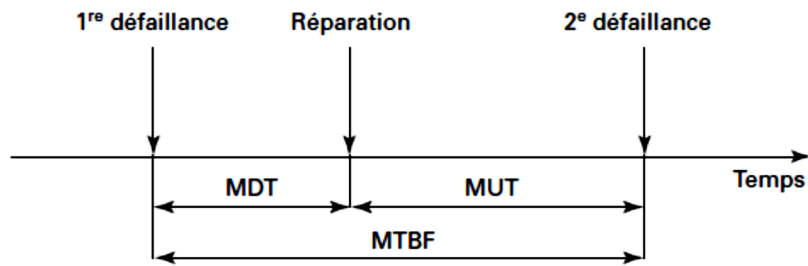


Figure 9 : Représentation des MTBF, MDT et MUT

Pour les industries disposant d'équipes performantes de maintenance, la valeur de A est supérieure à 80 %.

Exemple : Dans cette partie, on s'intéresse au temps de bon fonctionnement (TBF) d'une presse. A chaque panne, on associe le nombre de jours de bon fonctionnement ayant précédé de cette panne.

Les observations se sont déroulées sur une période de 4 ans et ont donné les résultats suivants :

Rang de la panne	1	2	3	4	5	6	7	8	9	10
TBF ayant precede la panne (en jours)	55	26	13	80	14	21	124	35	18	26

Calculer au jour près par défaut, le temps moyen de bon fonctionnement entre deux pannes

3.3 Maintenabilité (Maintainability)

Les défaillances étant par définition subies sans que l'on puisse prévoir leur instant d'apparition, il importe à tout responsable d'une installation industrielle de faire face rapidement aux conséquences d'une défaillance. Dans de nombreuses situations, sauf en cas de matériels redondants, il sera indispensable de réparer les défaillances dans un temps le plus court possible pour réduire les temps d'indisponibilité.

La compréhension des termes utilisés en maintenabilité rend nécessaire l'établissement d'un diagramme chronologique des temps entre l'instant de l'apparition de la défaillance et l'instant de la remise en service de l'installation. Le diagramme de la figure 10 résume tous les instants importants de cette chronologie.

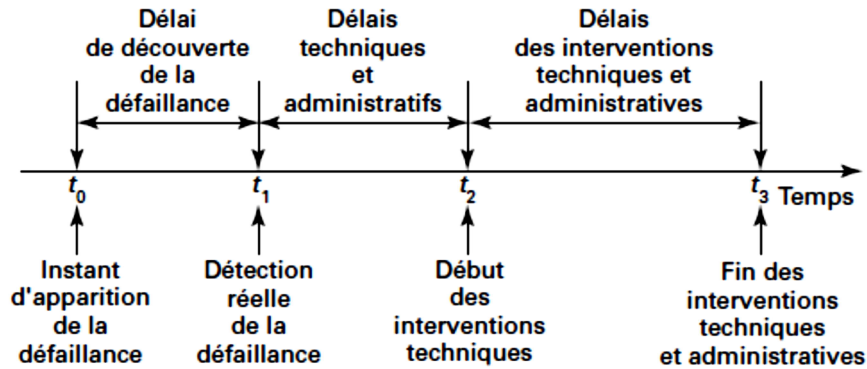


Figure 10 : Chronologie des temps des activités de maintenance

Dans cette séquence, l'instant t_0 correspond à l'instant de l'apparition réelle de la défaillance. En fonction des moyens mis à la disposition des opérateurs (systèmes d'alarme ou bien informations venant de rondes de surveillance), il s'écoulera un délai $t_1 - t_0$ allant de quelques secondes à quelques heures pour réaliser le diagnostic de la présence d'une défaillance. La confirmation de la défaillance ayant été réalisée, il s'écoule des délais techniques et administratifs pour réunir les personnels, les pièces détachées et les autorisations administratives (par exemple, consignation d'autres matériels) pour débiter les opérations de réparation. A partir du temps t_2 , les opérations de maintenance peuvent se dérouler et incluent également les procédures d'assurance qualité et l'obtention des autorisations administratives éventuelles (par exemple, pour les appareils à pression soumis à réglementation). Ce n'est qu'à partir du temps t_3 que l'on peut considérer que l'installation est devenue à nouveau opérationnelle.

d. Définitions de la maintenabilité

Suivant la norme AFNOR c'est : « dans les conditions données d'utilisation, l'aptitude d'une entité à être maintenue ou rétablie, sur un intervalle de temps donné, dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, avec des procédures et des moyens prescrits ».

On notera que la norme américaine MIL-STD-721C est presque identique dans sa formulation mais inclut le niveau requis de qualification des personnels :

« La maintenabilité est la mesure de l'aptitude d'un dispositif (« item ») à être maintenu ou remis dans des conditions spécifiées lorsque la maintenance de celui-ci est réalisée par des agents ayant les niveaux spécifiés de compétence, utilisant les procédures et les ressources prescrites, à tous les niveaux prescrits de maintenance et de réparation ».

La maintenabilité (maintainability) d'une entité réparable est caractérisée par une probabilité $M(t)$ que la maintenance d'une entité E accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t , sachant que E est défaillante au temps $t = 0$:

$$M(t) = P(\text{la maintenance de } E \text{ est achevée au temps } t)$$

$$= 1 - P(E \text{ non réparée sur la durée } [0, t])$$

Il s'agit donc d'un équivalent à la fiabilité mais appliqué à la réparation au lieu de la défaillance.

L'immaintenabilité correspond à la probabilité contraire, soit :

$$\overline{M(t)} = 1 - M(t)$$

La figure suivante représente l'allure de la maintenabilité $M(t)$ en fonction du temps.

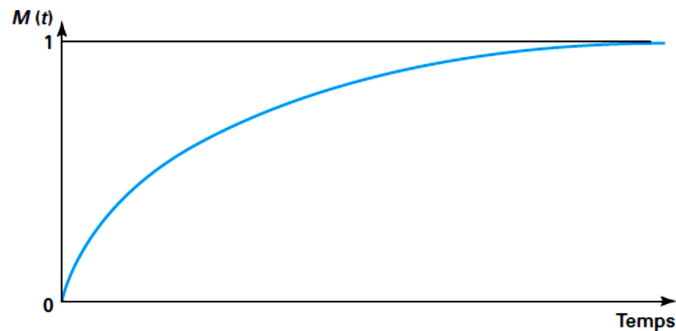


Figure 11 : Allure de la courbe de maintenabilité

On constate qu'à l'origine des temps $M(0) = 0$, ce qui est évident car l'entité est défaillante. Elle possède une asymptote égale à 1 car l'on peut supposer qu'elle sera réparée au bout d'un temps donné sinon cette entité ne serait d'aucune utilité.

e. Taux de réparation $\mu(t)$

On appelle taux de réparation $\mu(t)$ d'un système réparable au temps t la probabilité que l'entité soit réparée entre t et $t + dt$ sachant qu'elle n'était pas réparée sur l'intervalle $[0, t]$.

Elle se note :

$$\mu(t) = P(\text{entité réparée sur } [t, t + dt] \text{ sachant qu'elle n'était pas réparée sur } [0, t]).$$

$$\mu(t) = \frac{1}{1 - M(t)} \frac{dM(t)}{dt}$$

Pour obtenir un taux de réparation constant, il suffit de remplacer instantanément toute entité réparée par une nouvelle entité défaillante. Le taux de défaillance $\mu(t)$ est donc proportionnel au nombre de réparations relevées sur un intervalle de temps très court dt autour de t .

f. Intensité de réparation $g(t)$

A partir de la définition de la maintenabilité $M(t)$ on peut définir aussi l'intensité de réparation $g(t)$ représentant la densité de probabilité de la variable aléatoire correspondant au temps de réparation.

$$g(t) = \frac{dM(t)}{dt}$$

g. MTTR

Le terme MTTR (Mean Time To Repair) est la durée moyenne jusqu'à la réparation d'une entité réparable.

Pour cette variable aléatoire, le MTTR se calcule par la formule :

$$MTTR = \int_0^{+\infty} (1 - M(t)) dt$$

$$MTTR = \frac{\sum \text{Temps d'intervention pour n pannes}}{\text{Nombre de pannes}}$$

$$\mu = \frac{1}{MTTR}$$

Le MTTR s'assimile ainsi à la durée moyenne jusqu'à la première réparation et requiert la connaissance de l'état initial de l'entité. Comme il y a en général plusieurs modes de défaillances, il faut définir plusieurs MTTR d'une entité : à chaque mode de défaillance correspondra un MTTR spécifique.

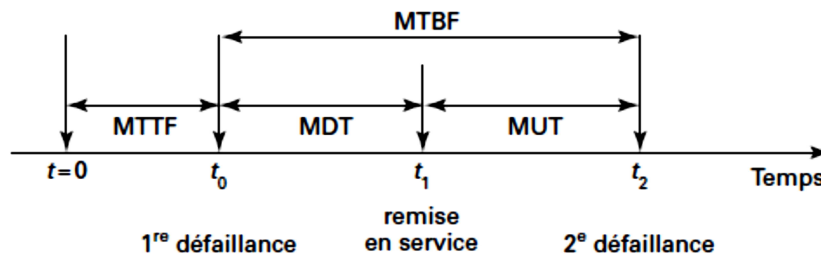


Figure 12 : Relations entre les liens temporels en fiabilité, disponibilité et maintenabilité

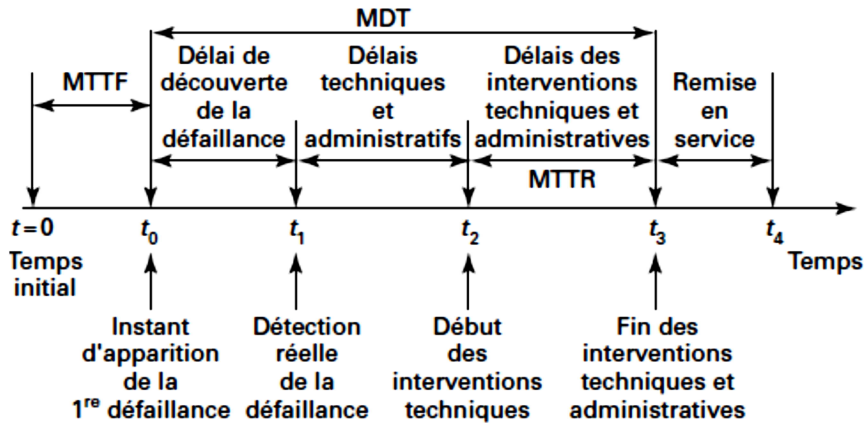


Figure 13 : Chaînage temporel des activités de détection et de remise en service

Les figures précédentes récapitulent les liens temporels entre les différents termes définis en fiabilité, disponibilité et maintenabilité.

Pour les systèmes existants, les performances en maintenabilité sont principalement dépendantes de la configuration des matériels et de leurs dispositions, des compétences et des organisations des équipes de maintenance (internes ou prestataires de service). L'expérience montre que, très souvent, les accès physiques aux pièces défaillantes sont difficiles. Il est utile de savoir que des normes définissent les espaces nécessaires pour réaliser les opérations de maintenance avec un opérateur humain.

3.4 Sécurité

La sécurité restant un terme très général, il n'existe pas actuellement de consensus pour une normalisation.

Le terme « security » concerne les aspects réglementaires de la sécurité (respects des normes, contrôle des accès à des locaux ou à des systèmes informatiques) tandis que le terme « safety » enseigné aux États-Unis sous le nom d'« industrial safety » recouvre les aspects techniques de la sécurité.

La Sûreté de fonctionnement est « l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques ».

Les circonstances et les conséquences des catastrophes et accidents sont variables. Elles montrent que le risque présente deux aspects : probabilité et conséquences. Au niveau des conséquences, celles-ci se caractérisent par la sécurité : protection des personnes, de l'environnement mais aussi protection de l'outil de production (aspect économique et, par extension, social).

Deux voies peuvent être pratiquées pour réduire les risques :

- diminution de la probabilité d'occurrence de « l'événement indésirable » ;
- atténuation des conséquences de « l'événement indésirable » ;

L'évaluation de la sécurité est actuellement encore limitée et est effectuée pour les installations chimiques, les centrales nucléaires, les plates-formes pétrolières et l'aéronautique. Elle est basée sur des études statistiques des impacts des accidents (réels, expérimentés ou simulés) sur l'homme et l'environnement (notion de gravité).

La démarche de la construction de la sécurité implique au départ la maîtrise des risques à un niveau acceptable, le risque zéro étant un concept qui ne peut se réaliser dans les systèmes industriels, contrairement à ce que de nombreux discours ou écrits ont tenté de le laisser croire, il y a seulement quelques années. Le niveau de risque acceptable prend en compte des paramètres techniques, économiques, médiatiques, sociaux voire politiques. Ces niveaux acceptables sont, pour des industries à risques, définis par les autorités administratives sous la direction des autorités ministérielles de tutelle. Ainsi, dans le domaine nucléaire, le risque acceptable pour la probabilité de fusion du cœur d'une centrale nucléaire est fixé dans la fourchette $10^{-5} - 10^{-6}$ par réacteur et par an pour la plupart des exploitants américains, européens et asiatiques.

Dans le domaine aéronautique, le risque de catastrophe aérienne est d'un accident par 10^7 vols.

Le rôle d'un spécialiste en Sécurité de fonctionnement est de ramener le risque industriel à son niveau acceptable en définissant :

- les critères d'acceptabilité des risques ;
- des méthodes de conception en sécurité ;
- des méthodes d'évaluation des risques résiduels et de vérification de leur niveau d'accessibilité.

Les études de sécurité visent essentiellement à évaluer la probabilité de l'occurrence d'un événement indésirable en prenant en compte dès la conception tous les facteurs initiateurs :

- facteurs techniques : matériels et produits manipulés (incluant les problèmes de conception, de fabrication, d'assurance qualité, de conduite et de maintenance) ;
- facteurs humains : qualité de la formation, ergonomie, procédures ;
- facteurs environnementaux : risques naturels, milieux ambiants (poussières, gaz, électricité statique...).

La figure suivante résume les liens entre fiabilité, maintenabilité, disponibilité et sécurité.

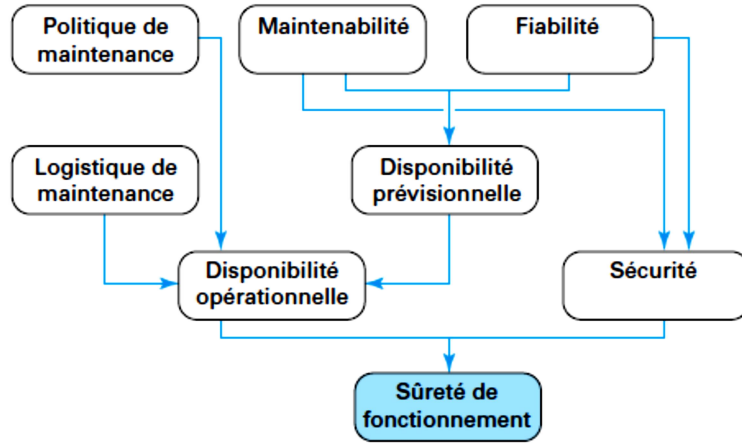


Figure 14 : Relations entre fiabilité, maintenabilité, disponibilité et sécurité

Chapitre 3

Calculs de fiabilité par structure

1. Principes

Le principe des calculs de fiabilité par structure (ou architecture) est de considérer qu'un système est constitué de composants élémentaires, et que sa fiabilité dépend à la fois de la fiabilité de ses composants et de la façon dont le bon fonctionnement ou la panne de chaque composant influe sur le bon fonctionnement ou la panne du système tout entier. Il est donc nécessaire de représenter la logique de fonctionnement du système.

Plusieurs types de représentations sont possibles : diagrammes de fiabilité, arbres de défaillance, graphes de Markov, réseaux de Petri, diagrammes de décision binaires, réseaux bayésiens, etc... On ne s'intéressera ici qu'à des systèmes non réparables et on représentera leur fonctionnement par un diagramme de fiabilité.

Le diagramme de fiabilité d'un système est un graphe sans circuit admettant une entrée E et une sortie S, dont :

- les sommets, appelés blocs, représentent les composants du système,
- les arcs traduisent les relations entre les différents composants, au sens où le système fonctionne si et seulement si il existe un chemin allant de E à S qui ne passe que par des composants en fonctionnement.

On peut faire l'analogie avec un réseau de distribution d'eau : l'eau n'est pas coupée tant qu'il existe un chemin dans le réseau qui lui permet d'aller de son point d'entrée à son point de sortie.

Remarque : le diagramme de fiabilité est une représentation logique du fonctionnement du système, qui n'a rien à voir avec une représentation physique des liaisons entre les différents composants. De même, il n'y a aucune contrainte de précédence dans ces diagrammes.

Exemple : une chaîne hi-fi comprend une platine CD (1), un tuner FM (2), un amplificateur (3) et deux enceintes (4 et 5). Le fonctionnement normal de la chaîne implique que tous ces

éléments fonctionnent. Le diagramme de fiabilité est alors donné dans la figure 12. En effet, si un seul de ces éléments ne fonctionne pas, la chaîne ne fonctionne pas correctement. Mais on peut admettre un fonctionnement dégradé dans lequel il est suffisant d'entendre au moins une des deux sources sonores sur au moins une des deux enceintes. Le diagramme de fiabilité est alors donné dans la figure 15.

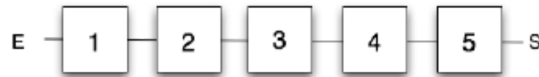


Figure 15 : Diagramme de fiabilité de la chaîne hi-fi en fonctionnement normal

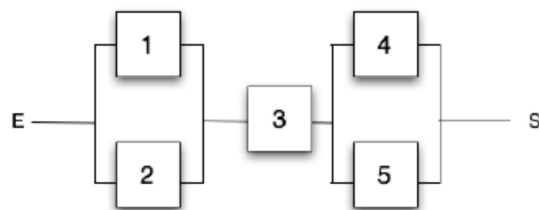
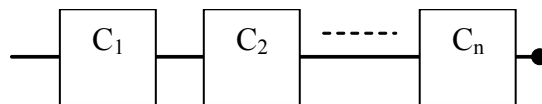


Figure 16 : Diagramme de fiabilité de la chaîne hi-fi en fonctionnement dégradé

2. Systèmes Séries

Un système constitué de n éléments sera dit « SERIE » au point de vue de la fiabilité, s'il est nécessaire que tous ses composants fonctionnent pour que le système fonctionne.



$$P(\text{systeme : fonctionne}) = P(C_1 : \text{fonctionne}) \times P(C_2 : \text{fonctionne}) \times \dots \times P(C_n : \text{fonctionne})$$

Si $R_i(t)$ est la fiabilité du composant i, et $R_s(t)$ la fiabilité du tous le système, on a :

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

a. Cas du modèle exponentiel

Si les composants C_i suivent un modèle exponentiel, $R_i(t) = e^{-\lambda_i t}$ alors :

$$R_s(t) = \prod_{i=1}^n e^{-\lambda_i t} = e^{-\sum_{i=1}^n \lambda_i t}$$

on pose : $\lambda_s = \sum_{i=1}^n \lambda_i$

d'où : $R_s(t) = e^{-\lambda_s t}$

b. Cas général

Dans ce cas $\lambda = \lambda(t)$ d'où : $R(t) = e^{-\int_0^t \lambda(t) dt}$

$$R_s(t) = \prod_i R_i(t) = \prod_i e^{-\int_0^t \lambda_i(t) dt} = e^{-\int_0^t \sum_i \lambda_i(t) dt}$$

Si on pose $\lambda_s(t) = \sum_{i=1}^n \lambda_i(t)$ on a : $R_s(t) = e^{-\int_0^t \lambda_s(t) dt}$

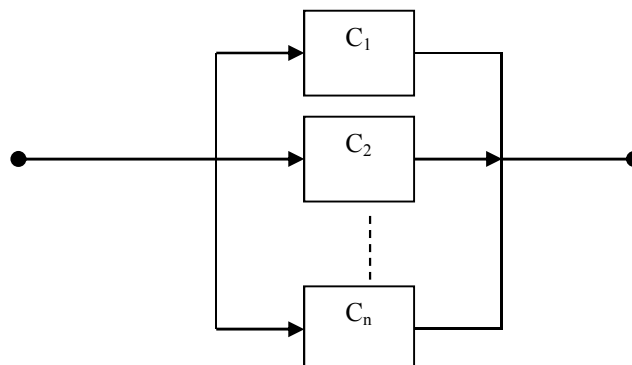
c. Calcul MTBF

$$MTBF = \int_0^{+\infty} R_s(t) dt$$

\Rightarrow $MTBF = \frac{1}{\sum_{i=1}^n \lambda_i}$

3. Systèmes Parallèles

Il est défini par le fait, qu'il faut que toutes les composantes C_i soient défailtantes pour que le système soit en panne.



La probabilité pour que le système soit en panne est donnée par :

$$P(\text{système en panne}) = P(C1 : panne) \times P(C2 : panne) \times \dots \times P(Cn : panne)$$

Donc

$$F_p(t) = \prod_{i=1}^n F_i(t) \quad \text{avec} \quad F_i(t) = 1 - R_i(t)$$

D'où :

Qu'on peut l'écrire :

$$R_p(t) = S_1 - S_2 + S_3 - \dots (-1)^{n+1} S_n$$

Avec:

$$\left\{ \begin{array}{l} S_1 = \sum_{i=1}^n R_i \\ S_2 = \sum_{i,j=1}^n R_i R_j \quad i \neq j \\ S_3 = \sum_{i,j,k=1}^n R_i R_j R_k \quad i \neq j \neq k \\ \vdots \\ S_n = \prod_{i=1}^n R_i \end{array} \right.$$

$$\underline{n=1}: \quad R_p = R_1$$

$$\underline{n=2}: \quad R_p = \sum_{K=1}^2 (-1)^{K+1} S_k = S_1 - S_2$$

$$S_1 = R_1 + R_2 \quad \text{et} \quad S_2 = R_1 \cdot R_2$$

$$R_p = R_1 + R_2 - R_1 \cdot R_2$$

$$\underline{n=3}: \quad R_p = \sum_{K=1}^3 (-1)^{K+1} S_k = S_1 - S_2 + S_3$$

$$S_1 = R_1 + R_2 + R_3$$

$$S_2 = R_1.R_2 + R_1.R_3 + R_2.R_3$$

$$S_3 = R_1.R_2.R_3$$

$$R_p = R_1 + R_2 + R_3 - R_1.R_2 - R_1.R_3 - R_2.R_3 + R_1.R_2.R_3$$

d. Cas du modèle exponentiel

Si les composants C_i suivent un modèle exponentiel, $R_i(t) = e^{-\lambda_i t}$ alors :

$$\left\{ \begin{array}{l} S1 = \sum_{i=1}^n e^{-\lambda_i t} \\ S2 = \sum_{i \neq j}^n e^{-(\lambda_i + \lambda_j)t} \\ \vdots \\ Sn = e^{-\sum_{i=1}^n \lambda_i t} \end{array} \right.$$

e. Calcul MTBF

Si les composants C_i suivent un modèle exponentiel, $R_i(t) = e^{-\lambda_i t}$ alors :

Pour $n = 2$

$$R_p = R_1 + R_2 - R_1.R_2$$

$$MTBF = \int_0^{\infty} R_p(t) dt$$

$$= \int_0^{\infty} (e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}) dt$$

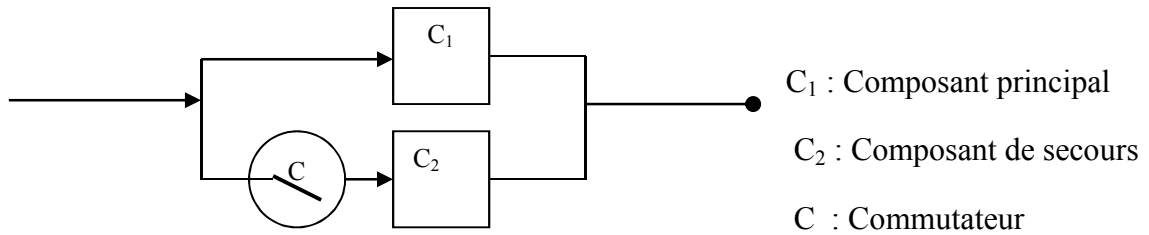
$$MTBF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2} - \frac{1}{\lambda_1 + \lambda_2}$$

Pour $n > 2$:

$$MTBF = \int_0^{\infty} R_p(t) dt = \int_0^{\infty} (S_1 - S_2 + S_3 + \dots + (-1)^{n+1} S_n) dt$$

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

4. Systèmes En « Stand By »



Le système fonctionne si on a 0 panne ou 1 panne

4.1 Cas d'une commutation parfaite

On admet que la fiabilité du commutateur est sensiblement égale à 1.

a) 1 « Stand by »

$$R(t) = Pr(0 \text{ ou } 1 \text{ panne})$$

Si l'occurrence de panne est « Poissonnienne »

$$Pr(X)_t = e^{-a} \frac{a^X}{X!} \quad \text{avec } a = \lambda t$$

Ce qui permet d'écrire

$$Pr(X)_t = e^{-\lambda t} \frac{(\lambda t)^X}{X!}$$

Donc on obtient :

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

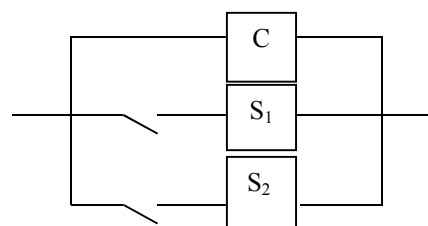
Dès lors

$$MTBF = \frac{1}{\lambda} + \frac{1}{\lambda} = \frac{2}{\lambda}$$

a) 2 « Stand by »

Ce système contient deux éléments de secours.

$$R(t) = Pr(0 \text{ ou } 1 \text{ ou } 2 \text{ pannes})$$



En appliquant la loi de Poisson :

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

$$MTBF = \frac{1}{\lambda} + \frac{1}{\lambda} + \frac{1}{\lambda} = \frac{3}{\lambda}$$

b) n « Stand by »

$$R(t) = Pr(0 \text{ ou } 1 \text{ ou } \dots \text{ ou } n \text{ pannes})$$

$$R(t) = e^{-\lambda t} \sum_{i=0}^n \frac{(\lambda t)^i}{i!}$$

$$MTBF = \frac{n+1}{\lambda}$$

Remarque : Si les composants ont des fiabilités différentes

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

$$MTBF = \frac{1}{\lambda_1} + \frac{1}{\lambda_2}$$

4.2 Cas d'une commutation imparfaite

On va tenir compte ici de la fiabilité du système de commutation R_C

$$R(t) = Pr(0 \text{ ou } 1 \text{ panne})$$

$$Pr(0) = e^{-\lambda t}$$

$$Pr(1) = e^{-\lambda t} \cdot \lambda t \cdot R_C$$

$$R(t) = e^{-\lambda t} \cdot (1 + \lambda t \cdot R_C)$$

$$MTBF = \frac{1 + R_C}{\lambda}$$

5. Redondance

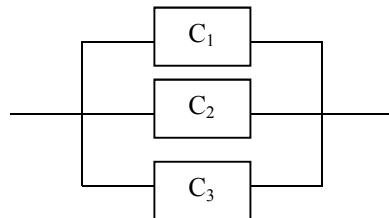
5.1 Caractéristique de la redondance

Une solution simple pour accroître la fiabilité d'un système est de mettre plusieurs composants, généralement identiques, en parallèle, soit :

- A. En redondance active : C'est à dire en faisant fonctionner tous les composants en même temps. (Cette technique est largement utilisée notamment sur les avions....)
Les éléments s'usent en même temps; mais une surveillance régulière de ces composants et le changement des défaillants sous perturbation pour le système permet d'atteindre de haut niveau de fiabilité.
- B. En redondance passive : dans laquelle on ne fait intervenir les éléments redondants qu'en cas de besoin, mais il faut alors un système de détection – commutation, c'est le « Stand by » déjà examiné.

Exemple : Redondance 2 parmi 3

Le système fonctionne lorsque au moins deux machines fonctionnent



$$R = R_1R_2R_3 + R_1R_2Q_3 + R_1Q_2R_3 + Q_1R_2R_3$$

Si les composants sont identiques :

$$R_{m/n}(t) = \sum_{k=m}^n C_n^k \cdot R^k \cdot (1-R)^{n-k}$$

5.2 Optimisation de la redondance

N ^{bre} de composants en parallèle	1	2	3	4	5	6
Fiabilité du système	0.8	0.96	0.996	0.9984	0.99968	0.999936
% d'accroissement par rapport à un seul composant		20%	24 %	24.8%	24.96%	24.99%

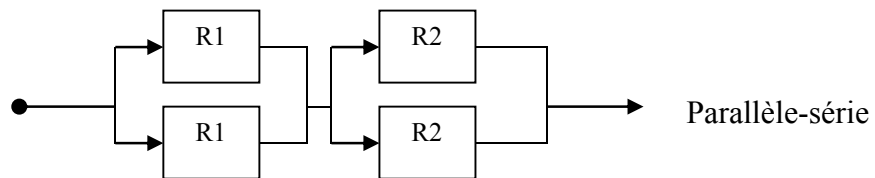
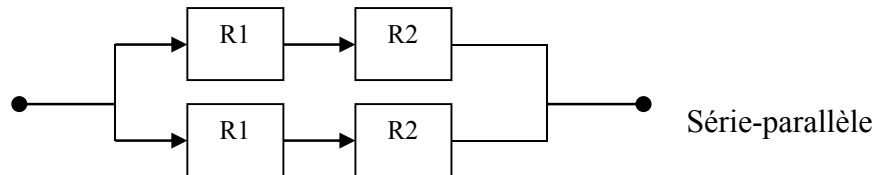
On remarque qu'à partir de la troisième redondance la fiabilité augmente légèrement. Donc on n'a pas d'intérêt d'augmenter le nombre de composant pour en avoir une faible augmentation de la fiabilité du système si le coût est très important

Il est intéressant d'examiner de plus près l'amélioration de la fiabilité de ces systèmes par redondance obtenue en doublant ou en triplant le nombre de composants

Soit un système série composé de deux machines on désire augmenter sa fiabilité en doublant ces composants.



Pour cela on propose deux dispositions dont on doit choisir celle qui donne la meilleure fiabilité.



On détermine alors la fiabilité de chacune, on a :

$$R_{ps} = [1 - (1 - R1)^2] \times [1 - (1 - R2)^2]$$

$$R_{sp} = 1 - (1 - R1 \cdot R2)^2$$

La différence des deux fiabilités montre que $R_{ps} > R_{sp}$

Donc on a intérêt de doubler composant par composant au lieu de doubler tout le système.

Chapitre 4 :

Méthodes d'analyse de sûreté de fonctionnement

Une analyse prévisionnelle de sûreté de fonctionnement est un processus d'étude d'un système réel de façon à produire un modèle abstrait du système relatif à une caractéristique de sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité, sécurité). Les éléments de ce modèle seront des événements susceptibles de se produire dans le système et son environnement, tels par exemple :

1. des défaillances et des pannes des composants du système,
2. des événements liés à l'environnement,
3. des erreurs humaines en phase d'exploitation.

Le modèle permet ainsi de représenter toutes les défaillances et les pannes des composants du système qui compromettent une des caractéristiques de SdF.

Afin d'aider l'analyste, plusieurs méthodes d'analyse ont été mises au point. Les principales sont :

1. APD Analyse Préliminaire des Dangers,
2. AMDE Analyse des Modes de Défaillances et de leurs Effets,
3. MDS Méthode du Diagramme de Succès,
4. MTV Méthode de la Table de Vérité,
5. MAC Méthode de l'Arbre des Causes,
6. MCPR Méthode des Combinaisons de Pannes Résumées,
7. MACQ Méthode de l'Arbre des Conséquences,
8. MDCC Méthode du Diagramme Causes-Conséquences,
9. MEE Méthode de l'Espace des Etats.

Nous ne verrons dans la suite que quelques unes de ces méthodes.

1. Premières méthodes

1.1 Analyse préliminaire des dangers

L'analyse préliminaire des dangers a été utilisée la première fois aux Etats-Unis dans les années 60 dans le cadre d'une analyse de sécurité de missiles à propergol liquide. Elle a ensuite été formalisée par l'industrie aéronautique et notamment pas le société Boeing. L'analyse se fait en phase amont de conception. L'objectif est d'identifier les dangers d'un système et leurs causes puis d'évaluer la gravité des conséquences liées aux situations dangereuses. L'identification des dangers est effectuée à l'aide de l'expérience et du jugement des ingénieurs, aidés de liste-guides élaborées dans des domaines précis et régulièrement enrichies. Les grandes étapes de cette analyse sont :

1. Identification du contexte opérationnel dans lequel évolue le système.
2. Identification des dangers potentiels et de la sévérité de leurs conséquences.
3. Définition d'actions correctives.
4. Vérification de la complétude de la liste des conditions de panne issue de l'analyse de risque et de compléter les exigences de sécurité. Fournit également les premières indications pour l'architecture du système afin de mitiger les conséquences.
5. Evaluation de l'atteinte des objectifs de SdF.

On illustre cette analyse avec un exemple extrait de l'ARP4761 (Aerospace Recommended Practice). On cherche à mettre des objectifs de sécurité sur le système de freinage.

Que doit-on évaluer ? Il faut d'abord identifier le système à évaluer, le contexte opérationnel, et les fonctions.

Avion, piste, contrôle de l'avion au sol

La description fonctionnelle de l'avion est la suivante.

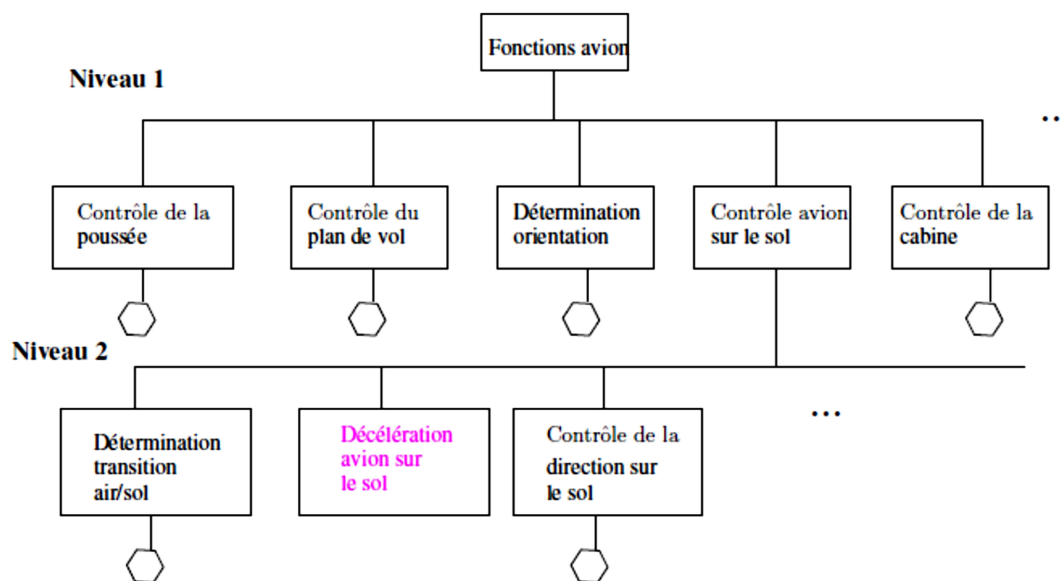
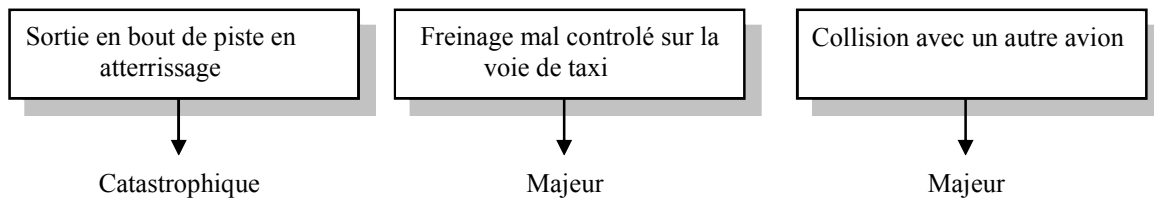


Figure 17 : Analyse fonctionnelle de l'avion

Que peut-il arriver? On identifie ensuite les dangers fonctionnels (dangers dus à de mauvaises performances des fonctions, ou à des problèmes contextuels)

Perte de la décélération sur la piste

A quel point cela est-il mauvais? On évalue les conséquences des dangers dans le pire cas.



A quelle fréquence est-ce acceptable? On détermine des objectifs de safety en terme de fréquence acceptable pour évènements ayant une certaine sévérité. (fh = flight hour)

catastrophique	$<10^{-9}/\text{fh}$
Hasardeux	$<10^{-7}/\text{fh}$
majeur	$<10^{-5}/\text{fh}$

Et on recommence. Il faut faire cette étude pour toutes les fonctions et tous les risques. Le résultat partiel de l'analyse est résumé dans le tableau suivant.

1. Fonction	2. Failure, Conditions Hazards	3. Phase, State Mode	4. Effects on Aircraft	5. Classification	6. Support	7. Verification
Decelerate aircraft on the ground	Loss of deceleration capabilities	Landing / RTO/ Taxi	See below			
	a) unannounced	Landing / RTO	Crew unable to decelerate, resulting in a high speed overrun	Catastrophic		FT
	b) annunciated	Landing	Crew selects a more suitable airport, prepares occupant for overrun	Hazardous	Emergency landing procedures	FT
	c) unannounced	Taxi	Crew unable to stop the aircraft, resulting low	Major		

			speeded contact with obstacles			
	d) annunciated	Taxi	Crew steers the aircraft clear for any obstacles and calls for a tug.	No safety effect		
	Asymmetric deceleration	Landing / RTO	See below			
	a) unannunciated	Landing / RTO	Offside excursion from the runway	Major		
	b) annunciated	Landing	Crew is prepared and counters with rudder and nose wheel steering input	Minor		
	c) Asymmetric deceleration	Taxi	Slightly diverts from intended course	No safety effects		

1.2 AMDE

La méthode d'Analyse des Modes de Défaillances et de leurs Effets a été employée la première fois dans les années 60 dans le domaine de l'aéronautique pour l'analyse de la sécurité des avions. Une AMDE (FMEA pour Failure Mode and Effects Analysis) est une analyse détaillée de toutes les défaillances simples, de leurs conséquences (ainsi qu'un chiffrage préliminaire de probabilité d'occurrence). Elle permet d'identifier les éléments critiques de sécurité (provoquant des événements critiques ou catastrophiques) ainsi que les fautes dormantes. En résumé, une AMDE permet :

1. d'évaluer les effets de chaque mode de défaillance des composants sur les fonctions du système,
2. d'identifier les modes de défaillances qui auront un effet important sur la sécurité, la fiabilité, la sécurité . . .

Considérons l'exemple représenté dans la figure suivante. Le système permet à un opérateur de commander le fonctionnement du moteur à courant continu; pour cela l'opérateur appuie sur un bouton pressoir (B.P.) provoquant ainsi l'excitation d'un relais, la fermeture du contact associé et l'alimentation électrique du moteur. Lorsque l'opérateur relâche la pression, le moteur s'arrête. Un fusible permet de protéger le circuit électrique contre tout court-circuit.

On suppose que le fil AB traverse une zone où se trouvent des vapeurs inflammables : on admet que l'analyse préliminaire des dangers a montré que l'évènement indésirable est la surchauffe du fil AB.

Le système est conçu pour faire fonctionner le moteur électrique pendant un temps très court ; on admet qu'un fonctionnement prolongé peut entraîner sa destruction par suite d'un échauffement du moteur et de l'apparition d'un court-circuit. On admet également qu'après l'apparition d'un courant élevé dans le circuit dû à un court-circuit, le contact du relais reste collé, même après la désexcitation du relais.

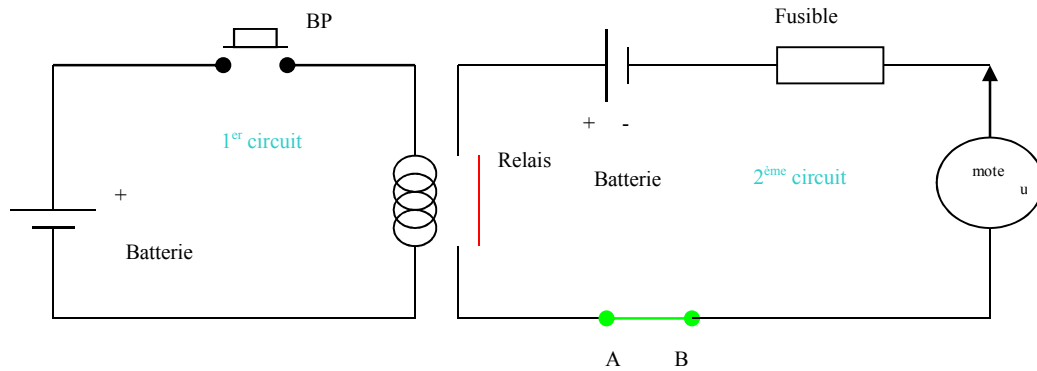


Figure 18 : Exemple d'illustration

L'analyse ne porte que sur le bouton-pressoir et le relais ; et on ne considère pour ces composants qu'un ou deux modes de défaillances.

Composant	Modes de défaillance	Causes possibles	Effets sur le système
BP	- Le BP est bloqué	- Défaillance mécanique	- Moteur ne tourne pas
	- Contact du BP bloqué	- Défaillance mécanique - Erreur humaine	- Moteur tourne trop longtemps: d'où court-circuit moteur et fusion fusible
Relais	- Contact bloqué ouvert	- Défaillance mécanique	- Moteur ne tourne pas
	- Contact collé	- Défaillance mécanique - Courant élevé dans le circuit	- Moteur tourne trop longtemps: d'où court-circuit moteur et fusion fusible

Tableau 5 : Exemple d'application de la AMDE

1.3 Diagramme de fiabilité

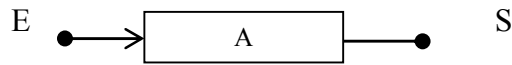
Historiquement, la méthode du diagramme de fiabilité ou de succès est la première à avoir été utilisée pour analyser les systèmes. Ses limites sont rapidement apparues, néanmoins elle permet de modéliser rapidement le système. On suppose dans la suite que le système n'est pas réparable.

Définition : Un diagramme de fiabilité est défini par :

- Une entrée E, un corps de diagramme et une sortie S
- Un flux est transmis de E jusqu'à S en passant par les différents chemins.
- Défaillance d'une entité arrête le flux au niveau du composant.

- S'il n'existe pas de chemin jusqu'à S, le système est défaillant, sinon il fonctionne.
- Configuration série ou/et parallèle.

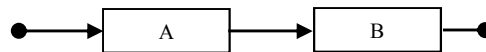
Les éléments, les fonctions, les événements extérieurs sont représentés par des blocs.



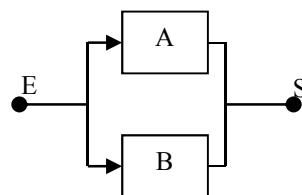
Règles de construction :

Cas simple : Système à 2 éléments A et B

Si la panne d'un seul élément met en panne le système alors on place en série les blocs correspondant à ces éléments

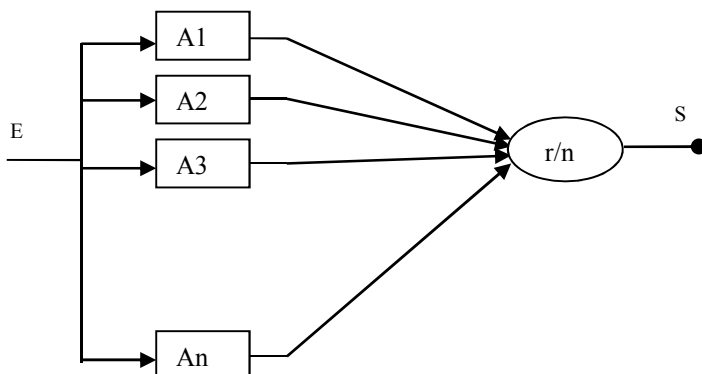


Si par contre, il faut que les 2 éléments soient en panne, pour que le système soit en panne alors on place les blocs.



Représentation redondance r / n

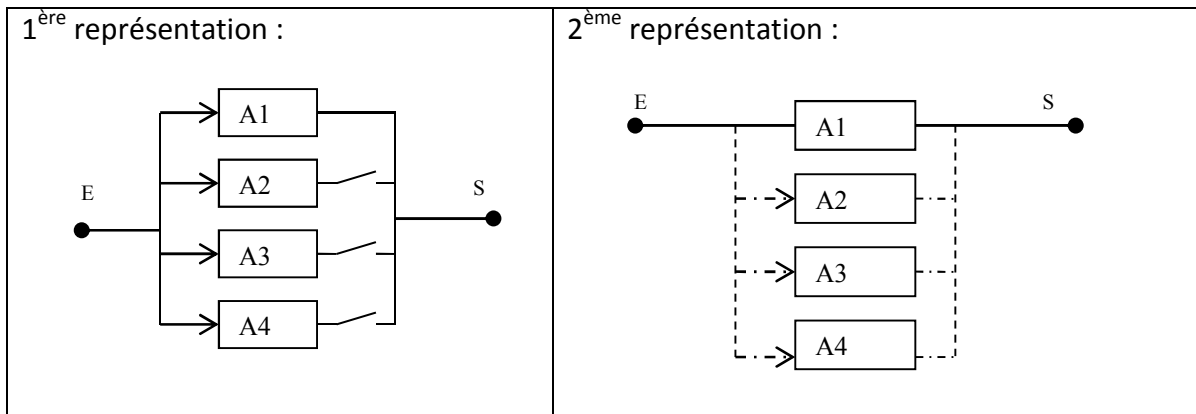
Au démarrage système, on a les n éléments en BF, mais le système continu à fonctionner tant qu'il existe au moins r éléments en BF.



Représentation des éléments en redondance passive

- Éléments en fonctionnement nominal (éléments principaux)
- Éléments secours (nominalement à l'arrêt) et qu'on ne fait démarrer que lors d'une panne d'un élément principal.

Systeme à 1 élément principal et 3 éléments secours



a. Analyse de systèmes complexes

Si le système n'est pas un assemblage de structures séries/parallèles, il faut adapter le calcul. Considérons l'exemple décrit ci-dessous.

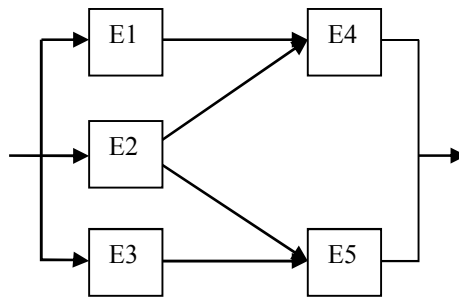


Figure 19 : Exemple de système complexe

Considérons les deux événements *le composant E2 fonctionne à l'instant t* et *le composant E2 est défaillant à l'instant t* de probabilité respectivement R_2 et $1-R_2$.

La fiabilité du système s'écrit alors :

$$R = P[S \text{ fonctionne à l'instant } t / E2 \text{ fonctionne à l'instant } t] \cdot R_2$$

$$P[S \text{ fonctionne à l'instant } t / E2 \text{ est défaillant à l'instant } t] \cdot (1 - R_2)$$

Si E2 fonctionne, S fonctionne si et seulement si E4 ou E5 fonctionne. Donc

$$P[S \text{ fonctionne à l'instant } t / E2 \text{ fonctionne à l'instant } t] = 1 - (1 - R_4)(1 - R_5).$$

Si E2 est défaillante, S fonctionne si et seulement l'une des deux séries E1.E4 ou E3.E5 fonctionne. Donc

$$P[S \text{ fonctionne à l'instant } t / E2 \text{ est défaillant à l'instant } t] = 1 - (1 - R_1 R_4)(1 - R_3 R_5).$$

$$\text{Finalement, } R = [1 - (1 - R_4)(1 - R_5)]R_2 + [1 - (1 - R_1 R_4)(1 - R_3 R_5)](1 - R_2).$$

b. Chemins – coupes

Un chemin à succès est un ensemble de blocs qui assurent la fonction. Dans l'exemple précédent, si Ei est assimilé à l'évènement Ei fonctionne à l'instant t , E1.E2.E4 est un chemin. Un chemin est dit minimal s'il ne contient pas d'autres chemins. Dans l'exemple précédent, les chemins minimaux sont E1.E4, E2.E4, E2.E5 et E3.E5.

Lorsque tous les chemins minimaux $\{L_i\}_{i=1..p}$ ont été identifiés, on obtient le résultat :

$$R = P\left(\sum_{i=1}^p L_i\right)$$

Dans l'exemple précédent, on a $R = P[E1.E4 + E2.E4 + E2.E5 + E3.E5]$.

A l'inverse, **une coupe** est une combinaison de défaillances qui conduit à la défaillance du système. Dans l'exemple précédent, $\bar{E}1.\bar{E}2.\bar{E}3$ est une coupe. Une coupe minimale est une plus petite combinaison de défaillances qui empêche d'aller de l'entrée à la sortie.

La connaissance des coupes minimales permet d'établir qualitativement la liste des composants critiques d'après l'organisation fonctionnelle du système. On appelle ordre d'une coupe le nombre d'éléments de la coupe. Lorsque toutes les coupes minimales $\{C_i\}_{i=1..n}$ ont été identifiées, on obtient le résultat :

$$\bar{R} = P\left(\sum_{i=1}^n C_i\right) = \sum_i P(C_i) - \sum_k (-1)^k \sum_{i_1}^{i_k} P(C_{i_1} \cap \dots \cap C_{i_k})$$

Si les probabilités sont très faibles, on approxime généralement la probabilité avec $\sum_i P(C_i)$.

Sinon, on encadre

$$\sum_i P(C_i) - \sum_{i=2}^n \sum_{j=1}^{i-1} P(C_i C_j) \leq \bar{R} \leq \sum_i P(C_i)$$

2. Arbres de défaillances

La méthode de l'arbre de défaillances, encore appelée arbre des causes (fault tree) est née en 1962 dans la société Bell Telephone grâce à Watson qui travaillait sur le projet Minuteman. Dans les années suivantes, les règles de construction ont été formalisées par Haasl en 1965, par l'University of Washington et Boeing. Dans les années 70, Vesely a jeté les bases de l'évaluation quantitative, Kinetic Tree Theory (KITTT). Enfin, en 1992, la dernière grande avancée est due à Coudert, Madre et Rauzy qui les ont codés avec des Diagrammes de décision binaires (DDB) obtenant ainsi une grande efficacité de calcul.

Cette méthode a pour objectif de déterminer les combinaisons possibles d'évènements qui entraînent l'occurrence d'un évènement indésirable (ou redouté). L'idée est de représenter graphiquement la logique de dysfonctionnement d'un système.

2.1 Construction d'un arbre de défaillance



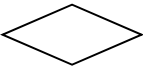
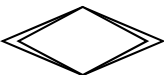




L'analyse par l'arbre de défaillance se concentre sur un évènement particulier qualifié d'indésirable ou de redouté car on ne souhaite pas le voir se réaliser. Cet évènement devient le sommet de l'arbre et l'analyse a pour but d'en déterminer toutes les causes.

On utilise généralement la convention du rond pour dénoter un évènement terminal, ou une feuille. Un évènement intermédiaire sera représenté par un rectangle. Quand un sous-arbre apparaît plusieurs fois, on peut factoriser l'écriture en utilisant les reports symbolisés par des triangles.

Dans le cas de la porte et, la sortie S est vraie si toutes les entrées E_i le sont. Pour la porte ou, la sortie S est vraie si au moins une des entrées E_i est à vrai. Dans le cas de la porte ou exclusif, la sortie S est vraie si une seule entrée est à vrai. Enfin, pour la porte k/n , S est à vrai si k évènements au moins sont à vrai sur les n .

Le schéma suivant est un guide permettant l'élaboration d'un arbre de défaillance. L'idée est de déterminer toutes les causes élémentaires qui mènent à l'évènement redouté.

2.2 Représentation des évènements

	rectangle	Représente un évènement qui résulte de la combinaison d'évènements plus élémentaires agissant à travers des portes logiques.
	Cercle	Représente un évènement de base
	Losange	Evènement supposé de base pour l'arbre considéré. En fait, cet évènement est subdivisible en évènements intermédiaires et de base. On fait pointer ce losange vers un autre arbre des causes.
	Double losange	Représente un évènement dont les causes ne sont pas encore développées, mais le seront ultérieurement
①  ② 	Triangle	La partie de l'arbre qui suit le symbole ① est transféré à l'endroit indiqué par le symbole ②. (Report)
①  ② 	Triangles inverses	Une partie semblable mais non identique à celle qui suit le symbole ① est transféré à l'endroit indiqué par le symbole ②. (Report)

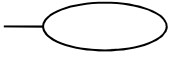
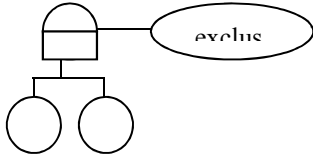

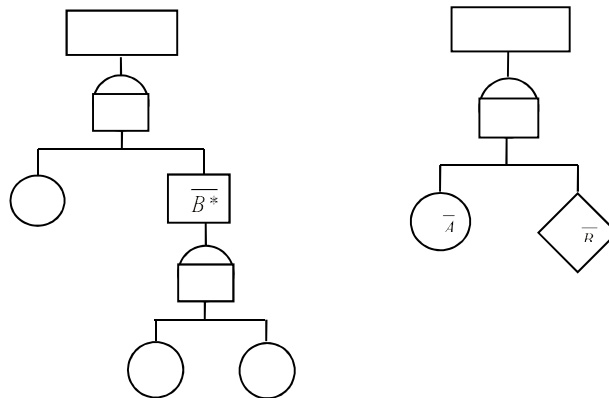


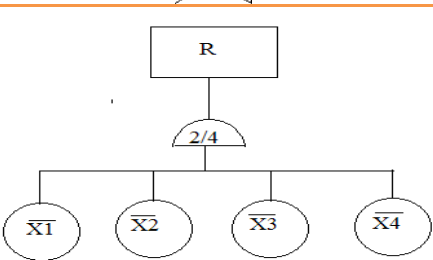
	<p>Condition</p>	<p>Représentation d'un évènement conditionnel, il est toujours associé à 1 porte logique. <i>Exemple :</i></p> 
	<p>Maison</p>	<p>Représente un évènement qui correspond à une utilisation normale du système.</p>

Tableau 6 : Représentation des évènements

Exemple :



2.3 Représentation des opérateurs logiques

Symbole	Type de porte
	Porte ET
	Porte OU
	Porte combinaison dès que l'on a combinaison d'au moins 2 ou 4 évènements alors qu'il y occurrence de l'évènements

	<p>résultant R Porte ET avec condition</p>
	<p>Porte OU avec condition</p>
	<p>Porte SI</p>
	<p>Porte délai : R apparaît 10 minutes après E1</p>
	<p>Porte matricielle On sait que R résulte de la combinaison des 4 événements mais ces combinaisons ne sont pas explicitées</p>
	<p>Porte quantification toujours en entrée de la porte sommation</p>
	<p>Porte sommation</p>

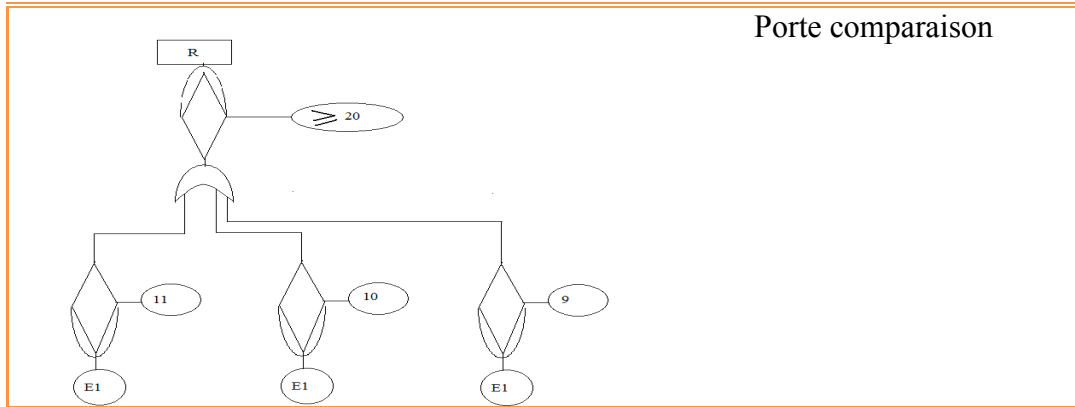
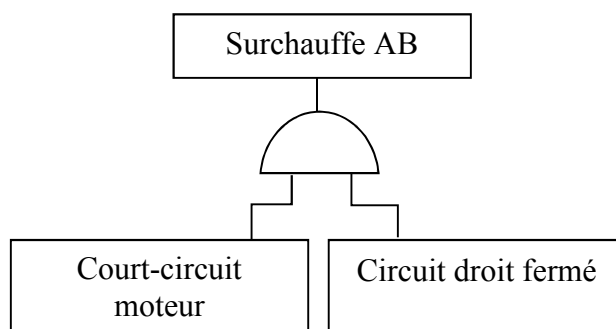


Tableau 7 : Représentation des Opérateurs logiques

Diagramme de fiabilité	Arbre de défaillance	Probabilité d'occurrence
		$P(\bar{S}) = P(\bar{E1} \cdot \bar{E2}) = P(\bar{E1}) \cdot P(\bar{E2})$ <p>(Si E1 et E2 sont indépendants)</p>
		$P(\bar{S}) = 1 - P(S)$ $= 1 - P(E1 \cdot E2)$ $= 1 - P(E1) \cdot P(E2)$ <p>(Si E1 et E2 sont indépendants)</p>

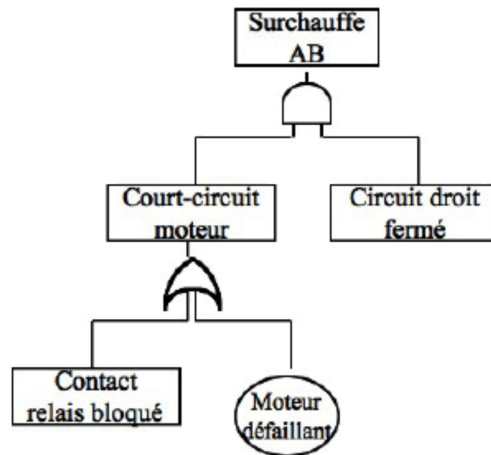
Tableau 8 : Equivalence Diagramme de fiabilité et Arbre de Défaillance

Exemple : On reprend l'exemple de la figure 15. L'évènement indésirable est la surchauffe du fil AB. Il ne peut résulter que de la présence d'un courant élevé dans le circuit de droite ce qui est le résultat d'un court-circuit du moteur et du fait que le circuit reste fermé. On en déduit l'arbre :



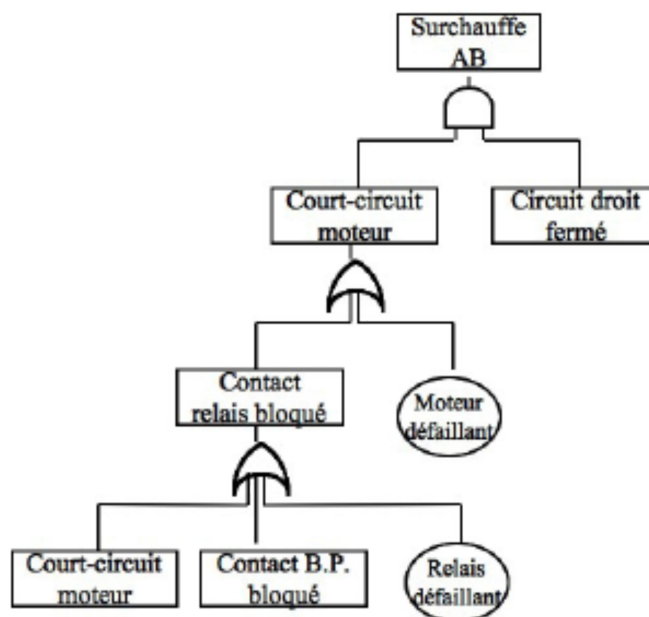
On recommence pour chaque évènement intermédiaire. Les causes du court-circuit moteur sont :

- soit une défaillance première du moteur (comme par exemple le vieillissement), c'est un évènement élémentaire ;
- soit le résultat d'une cause externe, ici ce sera le contact du relais resté collé.



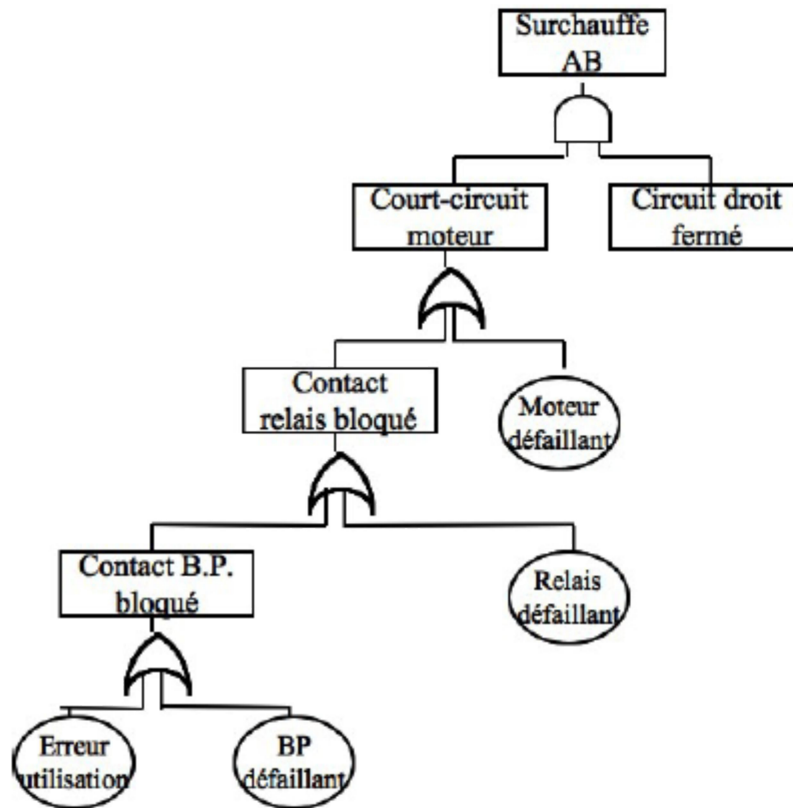
Les causes de l'évènement le contact du relais resté collé sont :

- soit une défaillance première du relais (comme par exemple une défaillance d'origine mécanique), c'est un évènement élémentaire ;
- soit le contact du relais reste collé si un courant élevé traverse le contact, c'est-à-dire s'il existe un court-circuit moteur ;
- soit le contact de B.P. reste collé.



On tombe sur un problème puisque le court-circuit moteur apparaît deux fois dans la même branche. Il faut donc supprimer cet évènement. Les causes de l'évènement le contact du B.P. resté collé sont :

- soit une défaillance première du BP (comme par exemple une défaillance d'origine mécanique), c'est un évènement élémentaire ;
- soit le contact du BP reste collé par suite d'une erreur humaine.



Enfin l'arbre complet est la suivant :

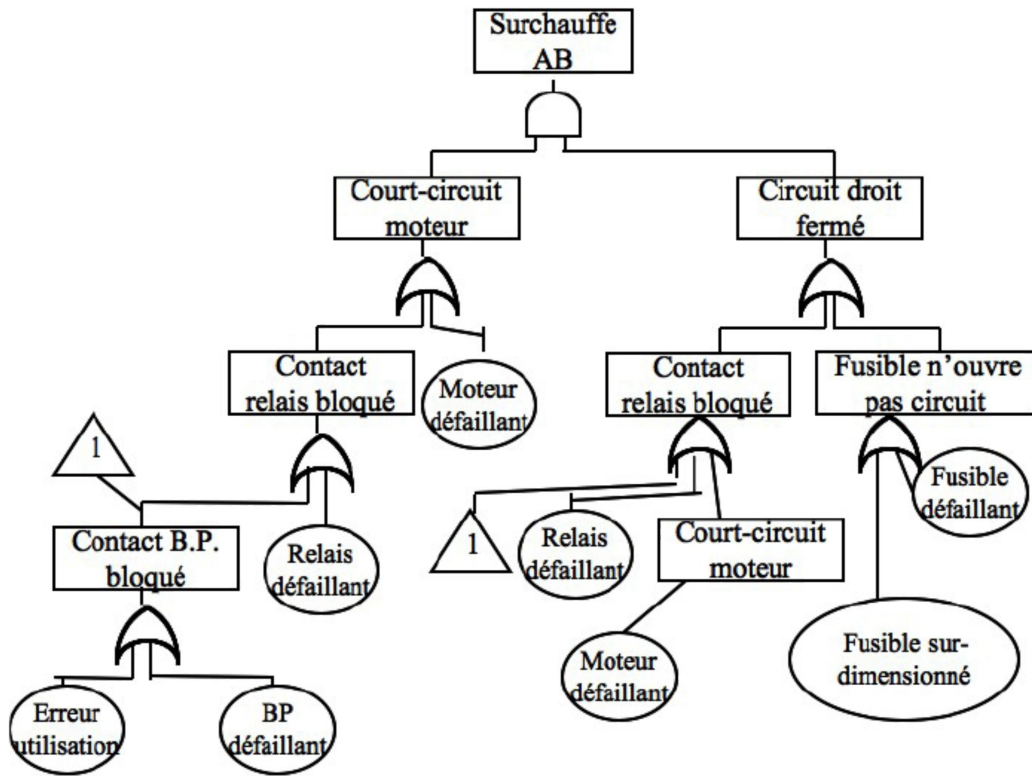


Figure 20 : Exemple d'arbre de défaillance

BIBLIOGRAPHIE

D. J. Smith, Fiabilité, maintenance et risque, Paris : Dunod /Usine nouvelle , 2006.

G. Zwingelstein, « Sûreté de fonctionnement des systèmes industriels complexes », Techniques de l'Ingénieur, S8250, 2009.

G. Zwingelstein, La maintenance basée sur la fiabilité. Guide pratique d'application de la RCM, Paris : Hermès, 1996.

P. Chapouille, « Fiabilité. Maintenabilité », Techniques de l'Ingénieur, T4300, 1980

Table des matières

Chapitre 1 : Introduction à la sureté de fonctionnement.....	1
1. Définition et Evolution de la discipline.....	1
2. Défaillances, fonctions d'un système et de ses composants.....	2
2.1 Définition de la défaillance fonctionnelle	2
2.2 Fonctions	5
3. Description des procédés industriels.....	6
3.1 Description générale.....	7
3.2 Description fonctionnelle.....	8
3.3 Description matérielle	8
Chapitre 2 : concepts de base de la sureté de fonctionnement.....	10
1. Rappels sur les probabilités	10
2. Loix de probabilité rencontrées dans les études de fiabilité	13
3. Concepts de base la sûreté de fonctionnement.....	15
3.1 Fiabilité (Reliability)	15
a. Densité de défaillance.....	16
b. Taux de défaillance	16
c. Moyenne de temps de vie avant la première défaillance (MTTF).....	18
3.2 Disponibilité (Availability)	18
3.3 Maintenabilité (Maintainability).....	20
d. Définitions de la maintenabilité.....	21
e. Taux de réparation $\mu(t)$	22
f. Intensité de réparation $g(t)$	23
g. MTTR	23
3.4 Sécurité	24
Chapitre 3 : Calculs de fiabilité par structure.....	27
1. Principes.....	27
2. Systèmes Séries	28
a. Cas du modèle exponentiel	28
b. Cas général.....	29
c. Calcul MTBF	29
3. Systèmes Parallèles.....	29
d. Cas du modèle exponentiel	31
e. Calcul MTBF	31
4. Systèmes En « Stand By ».....	32
4.1 Cas d'une commutation parfaite	32
4.2 Cas d'une commutation imparfaite.....	33
5. Redondance.....	34
5.1 Caractéristique de la redondance.....	34
5.2 Optimisation de la redondance	34
Chapitre 4 : Méthodes d'analyse de sureté de fonctionnement	36
1. Premières méthodes.....	37
1.1 Analyse préliminaire des dangers	37
1.2 AMDE	39
1.3 Diagramme de fiabilité.....	40
a. Analyse de systèmes complexes	42
b. Chemins – coupes	43
2. Arbres de défaillances.....	43
2.1 Construction d'un arbre de défaillance	44
2.2 Représentation des évènements.....	44
2.3 Représentation des opérateurs logiques.....	45
Bibliographie	51