Chapitre 1

Introduction à la sûreté de fonctionnement

1.1 Introduction

La sûreté de fonctionnement est l'ensemble des outils et méthodes permettant de

- caractériser et de maîtriser les effets des aléas, des pannes et des erreurs;
- quantifier les caractéristiques du dispositif ou des systèmes pour exprimer leur conformité dans le temps de leurs comportements et de leurs actions;
- analyser les causes de défaillance des composants pour estimer leurs conséquences sur le service rendu par le dispositif ou le système.

La sûreté de fonctionnement consiste à connaître, évaluer, prévoir, mesurer et maîtriser les défaillances des systèmes. Cette discipline a acquis ce nom et sa forme actuelle dans différents secteurs industriels en raison de sa corrélation avec la notion de qualité et les problèmes ergonomiques.

La sûreté de fonctionnement est appelée aussi 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). 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 en tenant compte des aspects probabilistes et des conséquences induites par les défaillances techniques et humaines.

La sûreté de fonctionnement est un moyen ou un ensemble de moyens : des démarches, des méthodes, des outils et un vocabulaire. Le but recherché de la sûreté de fonctionnement, est la maîtrise des risques.

L'analyse de la sûreté de fonctionnement permet de placer une confiance justifiée dans le système étudié. Cette confiance dépend de ce à quoi on accorde de l'importance et des valeurs relatives de ces caractéristiques.

1.2 Concepts généraux

Définition 1.1 (SdF) *La sûreté de fonctionnement d'un système correspond à son aptitude au maintien dans le temps de la qualité du service qu'il délivre.*

Il s'agit d'un concept global qui comprend principalement les caractéristiques de Fiabilité, de Maintenabilité, de Disponibilité, de Sécurité (FMDS), la durabilité... ou des combinaisons

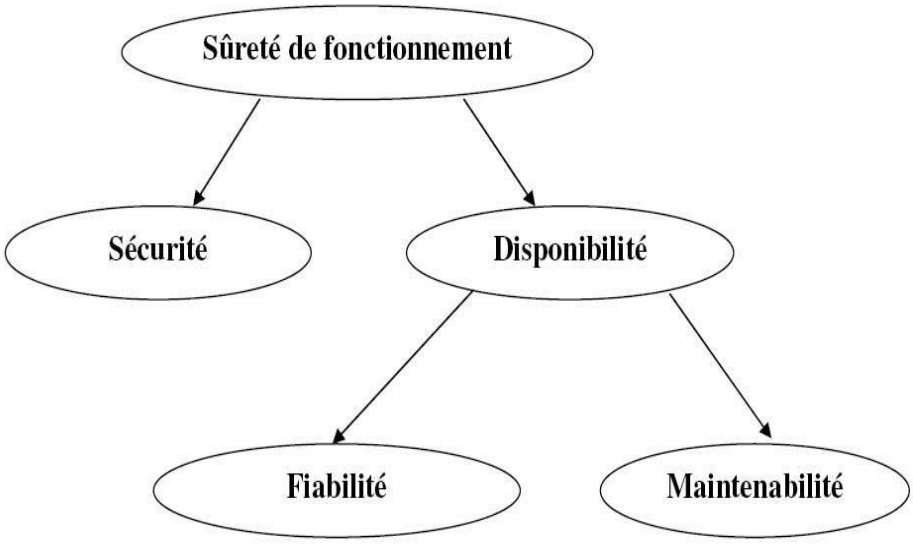

FIG. 1.1 – *Différents ingrédients de la SdF.*

de ces aptitudes. Au sens large, la SdF est considérée comme la science des défaillances et des pannes. Elle est basée essentiellement sur la disponibilité et la sécurité (voir figure 1.1).

Définition 1.2 *La sécurité est l'absence de dommages inacceptables. C'est la probabilité qu'une entité évite de faire apparaître, dans des conditions données, des événements critiques et catastrophiques.*

Par exemple dans le domaine informatique, la sécurité peut signifier :
- La sécurité-innocuité (Safety en anglais) vise à protéger des défaillances catastrophiques (exemple défaillance d'un disque dur).
- La sécurité-confidentiel (Security en anglais) correspond à la prévention d'accès ou de manipulation non autorisées de l'information.

La sécurité ne dépend pas obligatoirement de la fiabilité. En effet, un dispositif peut avoir une fréquence de défaillances faible mais lorsqu'il est défaillant, peut provoquer une panne sur un autre dispositif ou sur le système étudié.

Définition 1.3 *La disponibilité (Availability en anglais) est l'aptitude d'une antité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné. On note $A(t)$ cette disponibilité et on a:*

$$A(t) = Pr[E \text{ non défaillant à l'instant } t]$$

avec E un événement donné.

Pour atteindre le niveau de disponibilité, il faut trois ingrédients : la fiabilité, la maintenabilité et la logistique de maintenance. On définit la fiabilité de la manière suivante :

Définition 1.4 *La fiabilité (Reliability en anglais) est l'aptitude d'une entité à accomplir une fonction requise dans des conditions données et pendant une durée donnée. On note $R(t)$ cette fiabilité et on a :*

$$R(t) = Pr[E \text{ non défaillant sur } [0,t]]$$

avec E un événement donné.

Actuellement, il est primordial, dans un monde de compétitivité et de performance, d'introduire les effets de la fiabilité des dispositifs conçus. En effet des exigences de fiabilité sont couramment incluses dans les appels d'offre, ainsi que des pénalités en cas de non-respect de ces exigences.

La fiabilité du produit fabriqué permet de connaître son comportement en fonction de son utilisation. Après la construction d'un plan d'expérience des défauts, plusieurs actions peuvent être menées : la correction immédiate de défaut et la prise en compte du défaut dans la conception de nouveaux produits.

Dans le domaine de la production, la connaissance de la fiabilité des éléments les plus défaillants d'une machine de production est très importante. La nécessité de la production massive interdit les arrêts non prévus de la production à cause d'une panne. Grâce à un historique des pannes, la fiabilité de l'élément en cause pourra être calculée et ainsi en déduire une périodicité de changement. Ce dernier sera alors programmé au moment le plus favorable pour la production.

Définition 1.5 *La maintenabilité (Maintenability en anglais) est l'aptitude d'une entité à être rétablie dans un état dans lequel elle peut accomplir une fonction donnée (les conditions de maintenance étant prescrites). On note $M(t)$ cette maintenabilité et on a :*

$$M(t) = Pr[E \text{ est réparé sur } [0,t]]$$

avec E un événement donné.

La maintenabilité peut se traduire comme une caractéristique permettant d'assurer l'aptitude à la maintenance dans les meilleures conditions possibles. Elle doit être établie dans la perspective où elle est un élément fondamental, associée à la fiabilité, pour la construction de la disponibilité. Le déroulement de l'application de la maintenabilité peut être réparti en quatre étapes :

- l'allocation de maintenabilité,
- l'analyse des tâches et des moyens,
- les actions correctives éventuelles,

La maintenabilité s'est aussi :

- La mise en place des dispositifs de détection des défaillances qui permettent de suivre le bon fonctionnement des systèmes étudiés.
- Le choix des méthodes de diagnostic.

Définition 1.6 *La logistique de maintenance est la politique et les moyens de maintenance.*

Les principales politiques de maintenance sont basées sur :

- la maintenance corrective : la recherche systématique pour l'amélioration du matériel ;
- la maintenance préventive : ralentir le vieillessement d'un matériel, maintenir son niveau de performance;
- la maintenance currative : remettre en état de fonctionnement un matériel en panne.

La diminution de la durée d'intervention de la maintenance peut être atteinte grâce à :

- une meilleure accessibilité d'un élément dans un ensemble;
- la facilité de démontage et de remontage des éléments nécessitant des interventions fréquentes;
- l'interchangeabilité.

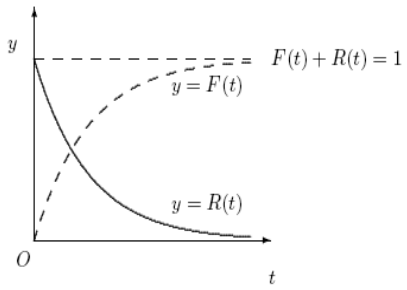

FIG. 1.2 – *Relation fiabilité-défaillance*

1.3 Taux de défaillance et de réparation

On commence tout d'abord par définir la notion de défaillance (voir figure 1.2).

Définition 1.7 *La défaillance (Failure en anglais) est la cessation de l'aptitude d'une entité à accomplir une fonction requise qui passe dans l'état de panne. On note $F(t)$ cette défaillance et on a :*

$$F(t) = 1 - R(t).$$

Les critères de défaillance sont définis selon différents types :
- par dérive ou dégradation,
- catalectique : défaillance complète et soudaine,
- totales, partielles, systématique, majeurs, mineurs, catastrophique,
- logiciels,
- humaines.

La figure (1.3) représente le diagramme de Farmer (1967). Elle met la relation entre la probabilité et la gravité et définit le risque comme le produit de la probabilité et la gravité :

$$\text{Risque} = \text{Probabilité} \times \text{Gravité}.$$

L'axe des abscisses qui correspond à la gravité des conséquences de l'événement redouté est décomposé selon le degré de gravité : mineur, significatif, critique et catastrophique.

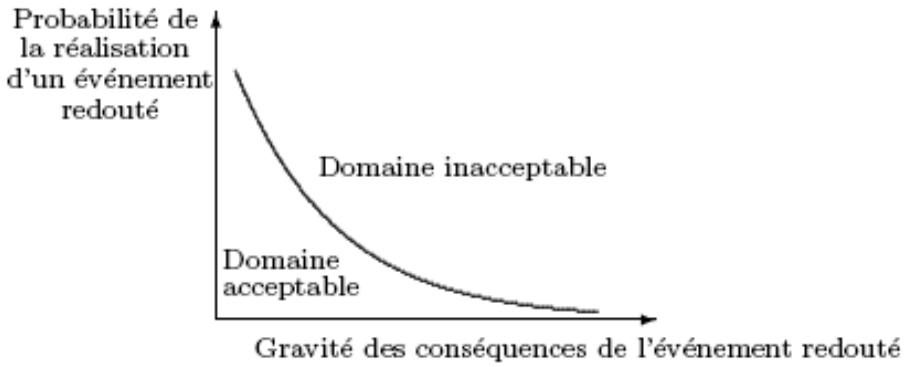

FIG. 1.3 – *Diagramme de Farmer*

L'approche de fiabilité permet d'introduire une mesure quantitative du risque de défaillance, au moyen d'une démarche probabiliste. Les méthodes quantitatives permettant d'analyser la sûreté de fonctionnement d'un système sont :
- l'Analyse Préliminaire des Risques (APR),

– la Méthode de l'Espace des États (MEE),
– les Arbres de Défaillances (AdD),
– le Diagramme de Fiabilité (DdF),
– l'Analyse de Modes de défaillances, de leurs Effets et de leurs Criticités (AMDEC).

On examine maintenant les différents indicateurs de la sûreté de fonctionnement.

Définition 1.8 *Le taux de défaillance est la limite, entre t et $t+dt$, du quotient de la densité de probabilité de défaillance par la probabilité de non défaillance avant t. Il est généralement noté $\lambda(t)$, et s'écrit sous la forme :*

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

$F(t)$ représente la probabilité d'apparition d'un défaut dans l'intervalle [0,t] et $R(t)$ représente la probabilité du succès à un instant t donné.

Soit T la variable aléatoire relative à la durée de fonctionnement de l'entité avant défaillance. On a donc

$$\lim_{t\to 0} F(t) = 0; \quad R(t) = Pr[T > t]; \quad R(0) = 1.$$

Et la fonction de répartition de la variable aléatoire T s'écrit

$$F(t) = Pr[T \leq t]; \quad \lim_{t\to+\infty} F(t) = 1.$$

La probabilité de défaillance $F(t)$ pour une période donnée est complémentaire à la fiabilité $R(t)$ du dispositif pour la même période considérée, on écrit alors

$$F(t) + R(t) = 1.$$

avec $R(0) = 1$ et $\lim_{x\to+\infty} R(t) = 0$.

La densité de probabilité de défaillance :

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

et $f(t)dt$ est la probabilité de défaillance de l'entité entre t et $t + dt$:

$$f(t)dt = Pr[t < T \leq t + dt]$$

d'où la fonction de répartition $F(t)$ s'écrit sous la forme

$$F(t) = \int_{-\infty}^{t} f(t).dt$$

$\lambda(t)dt$ est la probabilité de défaillance sur [t,t+dt] sachant que l'entité n'a pas eu de défaillance sur [0,t]. D'où

$$\lambda(t)dt = Pr[t < T \leq t + dt | T > t]$$

soit

$$\lambda(t)dt = \frac{Pr[(t < T \leq t + dt) \cap (T > t)]}{Pr[T > t]}$$

or $(T > t) \cap (t < T \leq t + dt) = (t < T \leq t + dt)$ donc

$$\lambda(t)dt = \frac{Pr[(t < T \leq t + dt)]}{Pr[T > t]}$$

d'où

$$\begin{aligned}\lambda(t)dt &= \frac{f(t)dt}{R(t)} \\ &= -\frac{dR(t)}{R(t)}\end{aligned}$$

d'où : $\int_0^t \lambda(x)dx = \int_0^t -\frac{dR(x)}{R(x)} = -\ln R(t)$, à $t = 0$ on a $R(0) = 1$. Donc la fiabilité s'écrit sous la forme suivante :

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

Dans le cas particulier où le taux de défaillance est constant, on a :

$$R(t) = e^{-\lambda t} \quad \text{et} \quad f(t) = -\frac{dR(t)}{dt} = \lambda e^{-\lambda t}.$$

Les modèles de prédiction de la fiabilité d'un dispositif sont déduit du temps de défaillance en se basant sur les recueils des données de l'expérimentation, les essais accélérés et le retour d'expériences. Pour évaluer la fiabilité d'un dispositif, il est nécessaire de savoir comment il devient défaillant dans le temps.

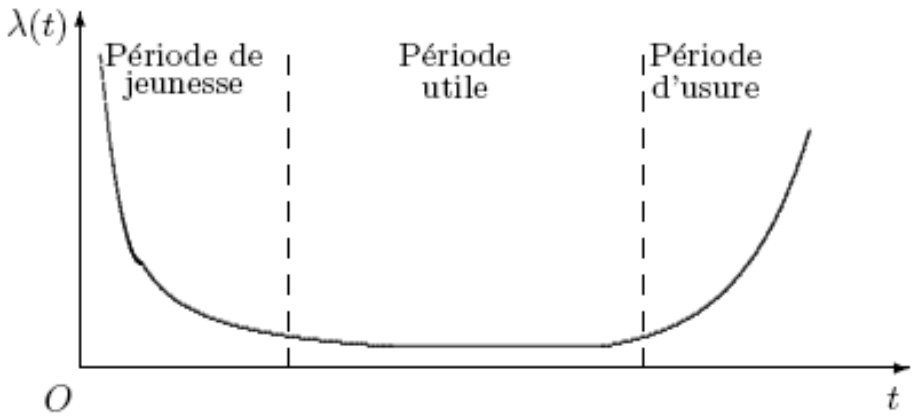

FIG. 1.4 – *Courbe en baignoire*

La courbe 3.1 se rencontre fréquemment dans le domaine mécanique. Elle fait apparaître l'évolution du taux de panne d'un équipement durant son cycle de vie. Il est à noter que cette courbe est découpée en trois zones : A, B et C.

Zone A : La première période qui suit la mise en marche d'un produit mécanique est dite "période de jeunesse". Elle est caractérisée par un taux de panne très important. Ce taux décroît peu à peu, car les défauts de rodage disparaissent. Un produit qui tombe en panne dans les jours qui suivent sa mise en service est donc tout à fait envisageable. Les défaillances sont dues à des défauts de fabrication ou à des phénomènes à évolution rapide. Cette période a une durée variable selon le produit. cette période peut être réduite par une mise sous tension des équipements en usine avant la livraison du produit c'est le déverminage.

Zone B : Cette période de croisière du produit relativement longue est caractérisée par un taux de panne constant, et le produit est donc robuste. Dans cette phase de maturité, la courbe est dans le bas de la "baignoire".

Cette période utile correspond à l'apparition de défaillance provenant des causes très diverses. Sa durée s'étend de quelques milliers d'heures pour les pièces mécaniques

à plusieurs centaines de milliers d'heures pour les composants électroniques selon le produit.

Zone C : Cette dernière période correspond au moment où les défaillances sont de plus en plus fréquentes, en raison du vieillissement et/ou de l'usure et de la fatigue. La courbe remonte brusquement.

On peut définir aussi le taux de réparation.

Définition 1.9 *le taux de réparation est la limite du quotient de la densité de probabilité d'achèvement de la répartition $m(t)$ entre t et $t + dt$, sur la durée $[0,t]$ de l'immobilisation. Il est généralement noté $\mu(t)$.*

On montre que ce taux relatif est égal au quotient de la dérivée, par rapport au temps, de la maintenabilité $M(t)$, par la probabilité complémentaire $1 - M(t)$:

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

Remarque 1.1 *Si on s'intéresse au point de vue du mécanicien. Si l'on prend comme exemple le coefficient de sécurité, on sait que ce dernier est égal à un rapport entre la résistance à la contrainte et la contrainte appliquée. Or, lorsque les mécaniciens font un calcul, ils ne s'intéressent pas à la répartition de la contrainte appliquée ou de la résistance à la contrainte, mais à la valeur moyenne de cette dernière. Cependant, dans la réalité, des hétérogénéités de matière, des imprécisions sur les dimensions ou autres font que la répartition de ces deux composantes peut être Gaussienne et avoir des dispersions relativement importantes. On verra plus en détail ces notions dans le chapitre 5.*

1.4 Estimateurs moyens

Couramment, on utilise les moyennes des temps du fonctionnement des systèmes, on commence par définir le MTTF :

Définition 1.10 (MTTF) *On appelle le MTTF (Mean Time To Failure) la moyenne des durées de fonctionnement de l'instant 0 à la première défaillance.*

Cette durée peut être calculée à l'aide des tests de durée de vie. Le MTTF est définie d'une manière générale de la façon suivante :

$$\begin{aligned} MTTF &= \int_0^{+\infty} t.f(t)dt \\ &= -\int_0^{+\infty} t.\frac{dR(t)}{dt}dt \\ &= [t.R(t)]_0^{+\infty} + \int_0^{+\infty} R(t)dt. \end{aligned}$$

À $t = 0$, $R(t) = 1$, d'où $t.R(t) = 0$. Quand t augmente, $R(t)$ décroît donc il existe k tel que $R(t) < e^{-kt}$ comme

$$\lim_{t \to +\infty} t.e^{-kt} = 0 \Rightarrow \lim_{t \to +\infty} t.R(t) = 0$$

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

Définition 1.11 (MTBF) *On appelle le MTBF (Mean Time Between Failure) la moyenne des temps qui sépare deux défaillances successives. Elle n'est définie que pour les systèmes réparables.*

Le MTBF peut être déterminé en testant le système pendant une période T et en comptant les défaillances N qui ont eu lieu.

$$\text{MTBF} = m = \frac{T}{N}$$

Cas particulier où λ est une constante

$$\begin{aligned} MTTF &= \int_0^{+\infty} e^{-\lambda t} dt \\ &= \left[-\frac{1}{\lambda} . e^{-\lambda t} \right]_0^{+\infty} \\ &= \frac{1}{\lambda} \end{aligned}$$

par conséquent

$$R(\text{MTBF}) = e^{-\lambda . MTBF} = e^{-\frac{MTBF}{MTBF}} = e^{-1} = 0{,}37.$$

Cela signifie qu'après un temps $t = \text{MTBF}$, approximativement 63% des composants en état de fonctionnement au début du test, tomberont en panne.

Remarque 1.2 *Le sigle MTBF, n'est équivalent au MTTF que pour une population d'entités à taux de défaillance constant. Le MTTF est défini pour les systèmes non réparables et le MTBF pour les systèmes réparables.*

Exemple 1.1 *A la suite d'un test de fiabilité de* 3000 *heures, effectué sur un lot de* 100 *pièces, on est arrivé aux résultats suivants :*

- *après* 1000 *heures : un défaillant,*
- *après* 2000 *heures : deux défaillants.*

On suppose $\lambda = cste$. λ est le nombre de défaillant par heure. Alors on calcule le MTBF de la façon suivante :

$$\lambda = \frac{3}{1000 + 2 \times 2000 + 97 \times 3000}$$

ce qui donne $MTBF = \frac{1}{\lambda} \approx 11$ ans.

Comme pour la défaillance, on associe à la réparation d'autres estimateurs, comme le MUT, le MTTR et le MDT.

Définition 1.12 (MUT) *On appelle MUT (Mean Up Time) le temps moyen de disponibilité, après réparation.*

Ce temps moyen est un peu inférieur au MTTF, car dans ce cas la réparation peut être partielle, notamment dans le cas de strutures redondantes, alors que le MTTF caractérise la durée moyenne de fonctionnement d'une entité complétement restaurée.

Définition 1.13 (MTTR) *On appelle le MTTR (Mean Time to Repair) la moyenne des temps techniques de réparation.*

Par définition : MTTR $= \int_0^{+\infty} t.m(t)dt$, ce qui donne :

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

Définition 1.14 (MDT) *On appelle le MDT (Mean Down Time) le temps moyen d'indisponibilité, après réparation.*