Généralités sur la Sûreté de Fonctionnement

I.1. Introduction

La sûreté de fonctionnement est une activité d'ingénierie qualitative et quantitative. La part qualitative correspond à l'optimisation des études au bureau d'études, elle représente 70% environ de l'activité totale. Les 30% restant représentent la partie dite quantitative qui est consacrée à la maîtrise des risques avant la fabrication à partir des architectures déjà élaborées. C'est donc la phase d'optimisation des architectures des systèmes et de leur mise en œuvre de façon à maximiser, à moindre coût, leur robustesse aux aléas.

La sûreté de fonctionnement est donc une action de réduction des risques et, par voie des conséquences, du coût à l'achèvement. Elle s'exerce donc essentiellement pendant les premières phases des projets, jusqu'à la mise en production.

Cette démarche est une partie de la démarche générale qui, depuis quelques années, est mise en œuvre pour contrôler la fabrication d'un produit ou d'un instrument donné, que l'on désigne sous le nom d'assurance produit.

I.2.But de la sûreté de fonctionnement

Le but de la sûreté de fonctionnement : mesurer la qualité de service délivré par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée.

Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système, mesurée par les grandeurs probabilistes associées : fiabilité, maintenabilité, disponibilité, sécurité.

I.3. Définitions - Abréviations

SdF : Sûreté de Fonctionnement (Dependability), aptitude d'une entité à satisfaire à une ou plusieurs fonctions requises dans des conditions données.

FMDS (RAMS) : Fiabilité, Maintenabilité, Disponibilité et Sécurité, acronyme pour désigner la sûreté de fonctionnement.

AFE (EFA) : Analyse Fonctionnelle Externe (External Functional Analysis), méthode visant à décrire de façon exhaustive les fonctions à réaliser pour satisfaire les besoins réels de l'utilisateur. Elle peut être également appelée Analyse Fonctionnelle du Besoin.

AFI (IFA) : Analyse Fonctionnelle Interne (Internal Functional Analysis), analyse visant à décrire comment les composants du système étudié participent à la réalisation des fonctions. Elle peut être également appelée Analyse Fonctionnelle Technique.

APR (PRA) : Analyse Préliminaire de Risques (Preliminary Risks Analysis), méthode visant à fournir l'ensemble des événements redoutés prévisionnels dans toutes les phases de vie du système étudié.

ADD (FTA) : Arbre De Défaillances (Fault Tree Analysis), outil destiné à déterminer les causes ainsi que la combinaison entre ces causes, qui pourraient conduire à la réalisation d'un événement redouté (ER).

AMDEC (FMECA) : Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (Failure Modes, Effects and Criticality Analysis). Méthode d'analyse d'un système qui comprend une analyse des modes de défaillance et de leurs effets, complétée par une analyse de criticité des modes de défaillance.

ER (RE) : Evénement Redouté (Risk Event), l'évènement redouté se définit comme la manifestation de la défaillance. Il s'exprime donc en termes de gêne pour le client.

Défaillance (Failure) : Cessation de l'aptitude d'une entité à accomplir une fonction requise.
Mode de défaillance (Failure Mode) : Manière de dont un système peut arrêter d'assurer ses fonctions. Il s'exprime en termes physiques (rupture, fatigue, coincement, fuite, court-circuit…), chimiques ou autres ayant entraînés une défaillance.

Durabilité (Durability) : Aptitude d'une entité à accomplir une fonction requise dans des conditions données d'utilisation et de maintenance, jusqu'à ce qu'un état limite soit atteint. Lorsque le système est réparable, l'état limite est au-delà duquel on ne répare plus.
Fonction défaillance F(t) (Unreliability) : La fonction défaillance représente la probabilité d'être défaillant avant un temps, kilométrage ou un nombre de sollicitations donné.

I.3 Qu'est-ce que la maintenance

I.3.1 Histoire

Le terme «maintenance » forgé sur les racines latines, Manus et Tenere est apparus dans la langue française au 12^{éme} siècle, l'étymologiste WACE à trouver la forme maintenance comme celui qui soutient, utilisée en 1169, c'est une forme archaïque de mainteneur.

Les utilisateurs anglo-saxons du terme sont donc postérieurs, à l'époque moderne, le mot a réapparu dans le vocabulaire militaire « maintien dans les unités de combat, de l'effectif et du matériel à des niveaux constant », définition intéressante, puisque l'industrie la reprise à son compte en l'adaptant aux unités de production affectées à un « combat économique »

Avant 1900 : on parle de réparation.

1900 - 1970 : on utilise la notion d'entretien, avec le développement des chemins de fer, de l'automobile, de l'aviation et l'armement pendant les 2 guerres mondiales.

A partir de 1970 : les développements de secteurs à risques et d'outils modernes aboutissent à la mise en œuvre de la maintenance.

Les principales raisons à retenir pour le passage de l'entretien à la maintenance :

- Automatisation.
- Evolution technologique.
- Amortissement.
- Contraintes réglementaires.
- Coût.

I.3.2 Coût de la sûreté de fonctionnement

Le coût d'un haut niveau de sûreté de fonctionnement est très onéreux. Le concepteur doit faire des compromis entre les mécanismes de sûreté de fonctionnement nécessaires et les coûts économiques.

Les systèmes qui ne sont pas surs, pas ables ou pas sécurises peuvent être rejetés par les utilisateurs. Le cout d'une défaillance peut être extrêmement élevé.

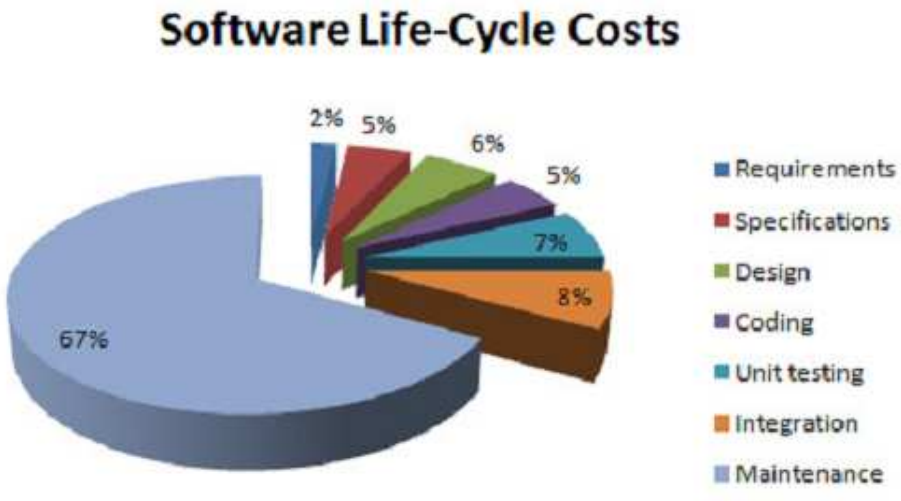


Figure I.1 : Cout de la maintenance.

I.4 Définition de la maintenance

La maintenance est << l'ensemble des activités destinées à maintenir ou à rétablir un bien dans un état ou dans des conditions données de sûreté de fonctionnement, pour accomplir une fonction requise. Ces activités sont une combinaison d'activités techniques, administratives et de management>>.

La maintenance est l'ensemble de toutes les tâches permettant de maintenir ou de rétablir un bien, dans l'état dans lequel il peut accomplir la fonction requise on appelle :

- **Bien :** Tout équipements «mécanique, électrique,……etc.» pouvant remplir une tâche bien définie dans la production de l'entreprise.
- **La fonction requise :** C'est la fonction ou ensemble de fonction d'un bien, considéré comme nécessaires pour un service donné

➢ **Selon l'AFNOR :** La maintenance est l'ensemble des actions permettant de maintenir ou de rétablir un bien dans un état spécifié, ou dans un état où il est en mesure d'assurer un service déterminé.

➢ **Selon LAROUSSE :** La maintenance est l'ensemble de tous ce qui permet de maintenir ou de rétablir un système en état de fonctionnement.

I.5 Les objectifs de la maintenance

I.5.1 Garantie la production prévue

La planification de la production doit être étudiée conjointement par l'entretien et la production en conciliant les arrêts nécessaires à l'entretien préventif et les recommandations du manufacturier tout en s'ajustant aux programmes de fabrication.

I.5.2 Amélioration de la qualité du produit

La qualité dépend autant de la production que de l'entretien; chacune de ces fonctions aura à rendre compte en cas de baisse de productivité de l'entreprise: erreur d'opération ou défaillance de la machine, matière première défectueuse ou de réglage de la machine, etc.

I.5.3 Contribuer au respect des délais

Il ya une double responsabilité au niveau de l'entretien: on doit connaître exactement l'état des équipements (pièces de rechange, historique des pannes, intervenants, caractéristiques techniques, stock pièces de rechange disponible etc.).

I.5.4 Recherche des coûts optimaux

Mis à part les compétences techniques, le service d'entretien doit être capable d'établir des devis précis et des estimés des coûts relié aux travaux de maintenance.

I.5.5 Assurance de la sécurité des travailleurs et la qualité du milieu de travail

Le service de maintenance doit se préoccuper des accidents que les interventions peuvent occasionner d'une part, pour ses propres tâches (méthode de travail, consignes de sécurité, cadenas sage, etc.).

I.5.6. Respecter l'environnement

Au service de maintenance incombe souvent le contrôle des polluants et le rejet des contaminants dans l'environnement. Il n'est pas rare que le matériel non productif mais nécessaire soit négligé (exemple: système de recyclage, dépoussiéreur, filtre, etc.).

I.6. Les différents types de Maintenance

- La maintenance corrective
- La maintenance préventive

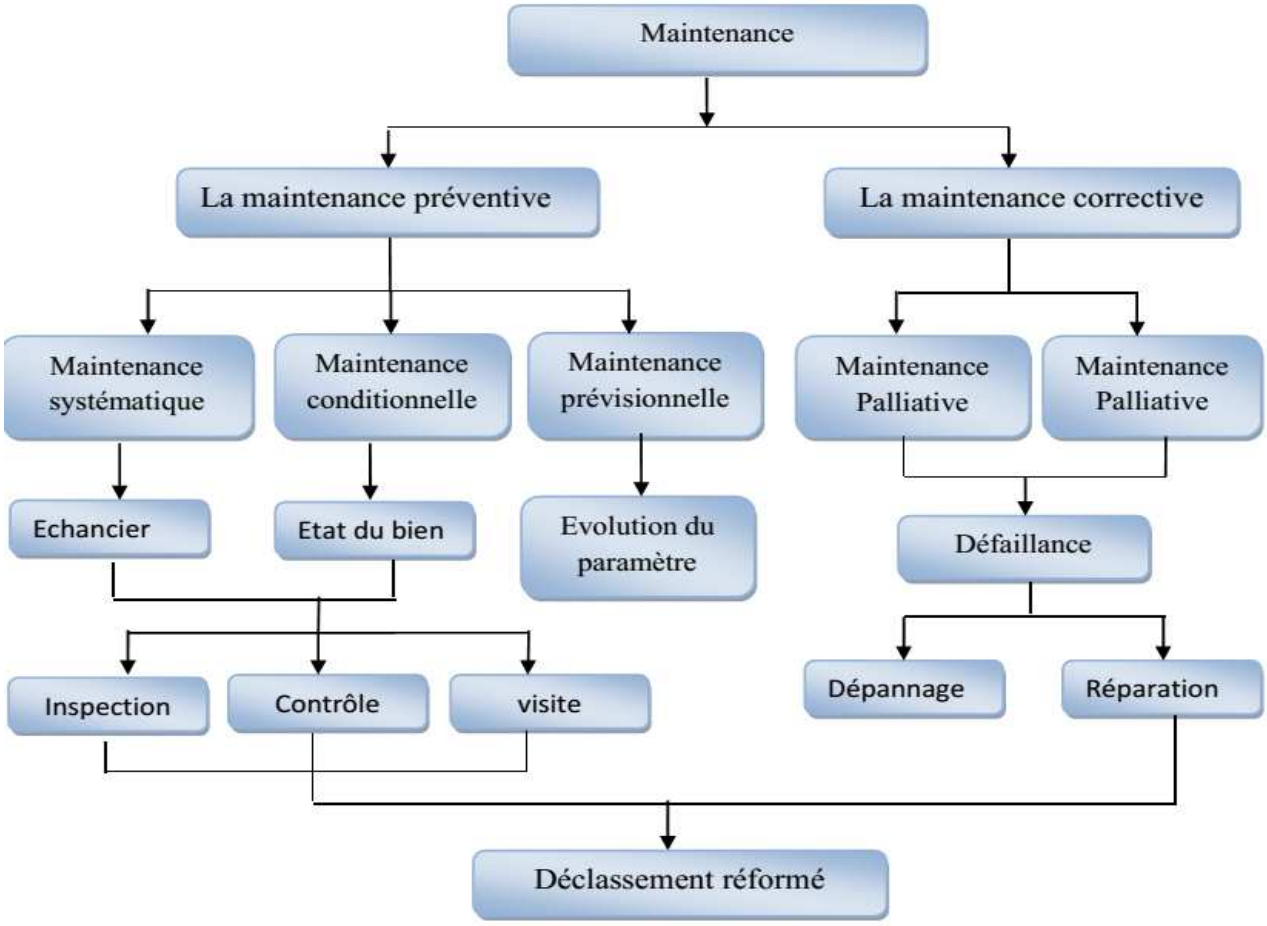


Figure I.2 : Organigramme types de maintenance.

I.6.1. La maintenance corrective

I.6.1.1. Définition

La norme AFNOR NF X 60 010 définit la maintenance corrective comme une maintenance effectuée après défaillance, où l'on distingue :

Le dépannage : action sur un bien en panne en vue de le remettre en état de fonctionnement.

Aussi, dans ce cas, il est indispensable de travailler méthodiquement. Une bonne préparation du travail, la saisie et la gestion de toutes les informations concernant les interventions de maintenance, permettront de terminer le travail en limitant les temps morts et en évitant les erreurs de démontage et de montage

On envisage deux types d'intervention :

- **Palliative** (dépannage), c'est-à-dire une remise en état de fonctionnement « caractère provisoire».
- **Curative** (réparation), c'est la réparation complète, parfois après dépannage « caractère définitif».

Cette maintenance est utilisée lorsque l'indisponibilité du matériel n'as pas de conséquences majeures sur le processus de production ou quand les contraintes de sécurité sont faibles.

I.6.1.2. Les opérations de maintenance corrective

Le dépannage

Actions physiques exécutées pour permettre à un bien en panne d'accomplir sa fonction requise pendant une durée limitée jusqu'à ce que la réparation soit exécutée.

Le dépannage n'a pas de conditions d'applications particulières. La connaissance du comportement du matériel et des modes de dégradation n'est pas indispensable même si cette connaissance permet souvent de gagner du temps.

Ainsi, le dépannage peut être appliqué par exemple sur des équipements fonctionnent en continu dont les impératifs de production interdisent toute visites ou intervention à l'arrêt.

La réparation

Actions physiques exécutées pour rétablir la fonction requise d'un bien en panne.

L'application de la réparation peut être décidée soit immédiatement à la suite d'un incident ou d'une défaillance, soit après un dépannage, soit après une visite de maintenance préventive conditionnelle ou Systématique.

Les révisions

Ensemble des actions et examens de contrôle et d'intervention effectuée en vue d'assurer le bien contre toute défaillance majeure ou critique, pendant un temps ou pour nombre d'unités d'usage donnée.

I .6.2. La maintenance préventive

I .6.2.1. Définition

Définition AFNOR (X-60-010):Maintenance effectuée dans l'intention de réduire la probabilité de défaillance d'un bien ou la dégradation d'un service rendu.

I .6.2.2. Les types de maintenance préventive

- ✓ La maintenance préventive systématique.
- ✓ La maintenance préventive conditionnelle.

A) La maintenance préventive systématique

a) Définition

AFNOR X-60-010 :« Maintenance préventive effectuée suivant un échéancier établi, suivant le temps ou le nombre d'unité d'usage».

Cette maintenance comprend des inspections périodiques et des interventions planifiées.

b) Avantage

C'est une maintenance facile à gérer car les périodes d'interventions sont fixes, elle permet :

- d'éviter les détériorations importantes.
- de diminuer les risques d'avaries imprévues.

c) Inconvénient

Reposer sur la notion de MTBF et ne prends pas en compte les phénomènes d'usure.

B) La maintenance préventive conditionnelle

a) Définition

AFNOR X-60-010 : « Maintenance préventive subordonnée à un type d'événement prédéterminé révélateur de l'état du bien. »

b) avantages

- elle sécurise : détection de l'arrivée des défauts.
- elle améliore la disponibilité par la planification des opérations.
- elle favorise les facteurs humains (appel aux compétences des opérateurs).

c) inconvénients

- Pour être efficace elle doit être pensée dès la phase de conception.

I.6.2.3. Les opérations de maintenance préventive

- ❖ **Inspection**

C'est l'activés de surveillance consistant à relever Périodiquement des anomalies, et d'exécution de réglages simples ne nécessitant pas d'outillage spécifique ni l'arrêt des équipements.

- ❖ **Le contrôle**

Vérifications de conformité par rapport à des données préétablies suivies d'un jugement. Le contrôle peut :

- Comporter une activité d'information ;
- Inclure une décision : acception, rejet, ajournement ;
- Déboucher comme les visites sur des opérations de maintenance corrective.

Les opérations de surveillance (contrôles, visites, inspections) sont nécessaires pour maitriser L'évolution de l'état réel du bien. Elles sont effectuées de manière continue ou à des intervalles Prédéterminés ou non, calculés sur le temps ou le nombre d'unités d'usage.

❖ **La visite**

C'est l'opération de surveillance de maintenance préventive systématique qui s'opère selon une périodicité prédéterminée. Ces interventions correspondent à une liste d'organes et une immobilisation du matériel.

I.7 Les concepts de base de la sureté de fonctionnement (SDF)

La sûreté de fonctionnement (SDF) 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), FMD (Fiabilité, Maintenabilité, Disponibilité), en anglais RAM (Reliability, Availability, Maintainability). 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.

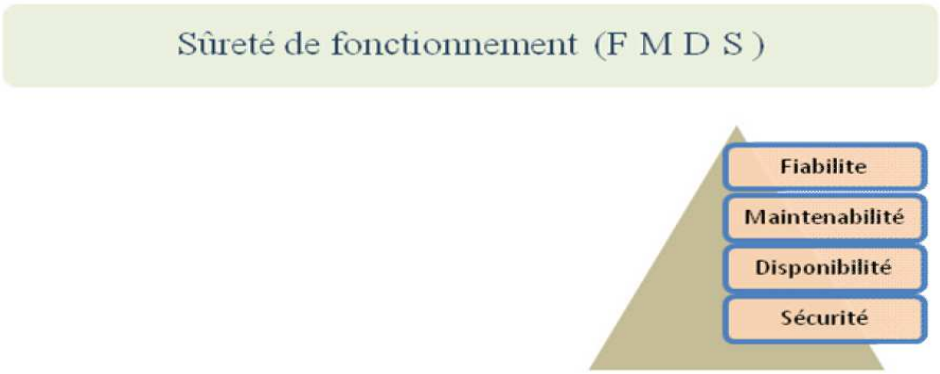


Figure I.3 : Concept de la FMDS.

I.7.1. Fiabilité

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 non-défaillante sur la durée [0, t], en supposant qu'elle n'est pas défaillante à l'instant t = 0). Ce qui peut s'exprimer par:

R (t) = P (T > t)

L'aptitude contraire est appelée dé fiabilité, et est définie par :

F(t)=1-R(t)= P(t<T)

On distingue plusieurs types de fiabilité (termes spécifiques) :

I.7.1.1. Les différents types de fiabilité

- **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.

I.7.1.2. Analyse de la fiabilité

Selon la **loi de Weibull** qui est une loi continue à être utilisée le long du cycle de vie d'un matériel, les fonctions de la fiabilité dépendent de trois paramètres: β, γ, η Caractérisent ce modèle.

- **Densité de probabilité**

Elle caractérise la probabilité de panne juste à temps.

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

- **La fonction de répartition**

Elle représente la probabilité des pannes cumulée de défaillance entre 0 et t

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

- **Le taux de défaillance**

C'est la probabilité instantanée d'une panne au temps (t + Δt), sachant que mon dispositif est bon à l'instant t. $\lambda(t) = \frac{f(t)}{R(t)} = \frac{\beta}{\eta}\left[\frac{1-\gamma}{\eta}\right]^{\beta-1}$

Figure I.4 : Performance et défaillance d'un dispositif.

- **Le moyen de temps de bon fonctionnement MTBF**

C'est la racine de temps de bon fonctionnement [MTBF] divisée par le nombre des pannes. MTBF = γ+A η

❖ Signification des déférents paramètres de la loi de Weibull

Paramètre de forme β

Ce paramètre donne l'allure de la distribution des défaillances, il est sans dimensions

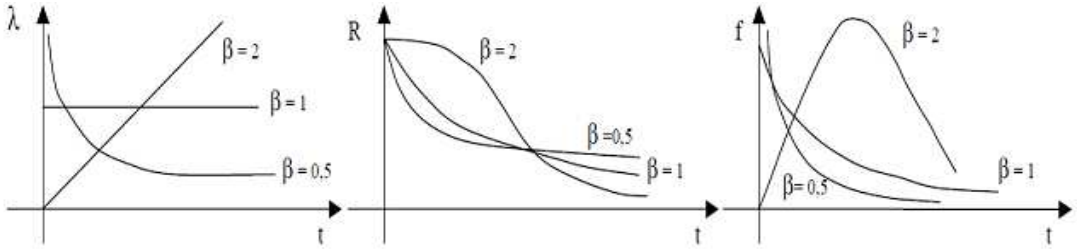


Figure I.5 : Les trois périodes de la courbe en baignoire avec différentes valeurs de β

Courbe de défaillance

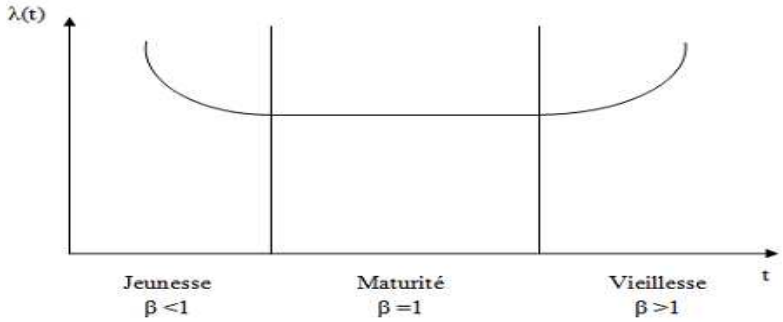


Figure I.6 : Allure d'un taux de défaillance « en baignoire » .

β <1 :

Correspond à la zone décroissante de la courbe, c'est la période de mise en place de rodage de l'installation (période de jeunesse).

β =1 :

Corresponde à la zone ou le taux de défaillance est pratiquement constant, c'est la période de défaillance aléatoire qui ne présente généralement avec un symptôme de dégradation préalable (vie utile). C'est la période la plus longue.

β>1 :

Corresponde à la zone croissante rapide, c'est la période de vieillesse provoqué par l'usure mécanique.

Paramètre de position γ

Son unité est celle de la variable, il explique la survie du lot .

Si $\gamma < 0$ dès la réception du matériel, il y a défaillance.

Si $\gamma > 0$ il y a survie totale du lot.

Paramètre d'échelle η

En unité de temps qui est associé à l'échelle utilisée sur le graphe d'ALAIN PLATT.

Ce dernier qui est en papier de WEIBULL utilise la méthode graphique pour l'estimation des

Paramètres de cette loi. Il est gradué comme suit :

- En abscisse: ln(t)
- En ordonnées :$\ln(\ln(\frac{1}{1-F(1)}))$

I.7.2. La Maintenabilité

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 I.7) résume tous les instants importants de cette chronologie.

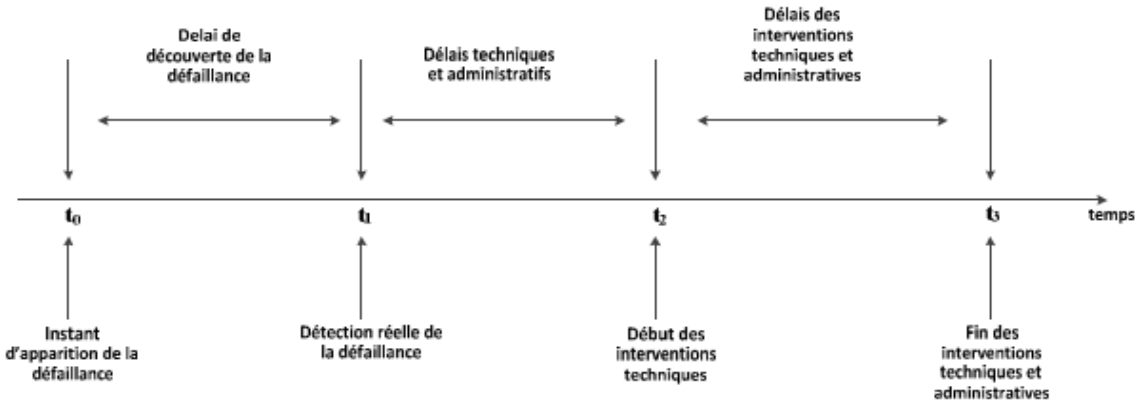


Figure I.7 : Chronologie des temps des activités de maintenance .

I.7.2.1. Définition de la maintenabilité

(AFNOR X-06-010) : «Aptitude d'un dispositif à être maintenu ou rétabli dans un état dans lequel il puisse accomplir une fonction requise lorsque la maintenance est

accomplie dans des conditions d'utilisation données avec des moyens et procédures prescrits».

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.

La maintenabilité est la mesure de l'aptitude d'un dispositif (« item ») à être maintenu ou remis dans des conditions spécifies 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 d′un équipement dépend essentiellement de la facilité de démontage de ces éléments consécutifs et de leurs interchangeabilité.

- Maintenabilité intrinsèque.
- Maintenabilité extrinsèque.

I.7.2.2. La fonction maintenabilité

C′est la probabilité pour qu′un dispositif soit répare avant (t).

$$M(T) = 1 - e^{-\mu.t}$$

M (t) : est constant alors μ : taux de réparation.

I.7.3. La disponibilité

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 non-défaillante à l'instant t).

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

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

C'est L'aptitude d'un dispositif à être en état de fonctionnement dans ces conditions données sous les aspects combines de la fiabilité de la maintenance, la logistique et l'organisation de maintenance c'est la probabilité pour qu'un dispositif soit en état de fonctionnement selon des conditions de maintenance prescrite et pour un temps donné.

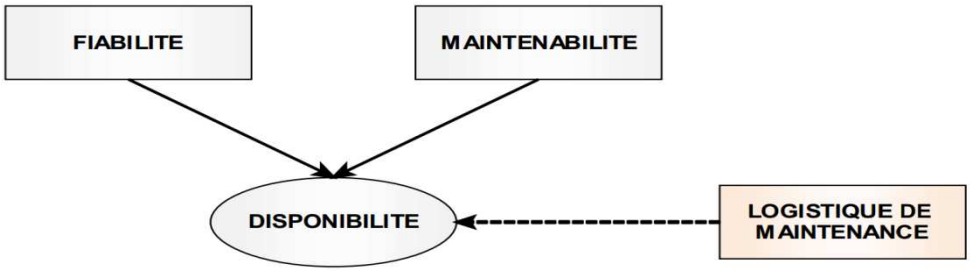


Figure I.8 : La disponibilité.

Remarque : 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.

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

—**Disponibilité instantanée** prévisionnelle (définie précédemment);

—**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 .

(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

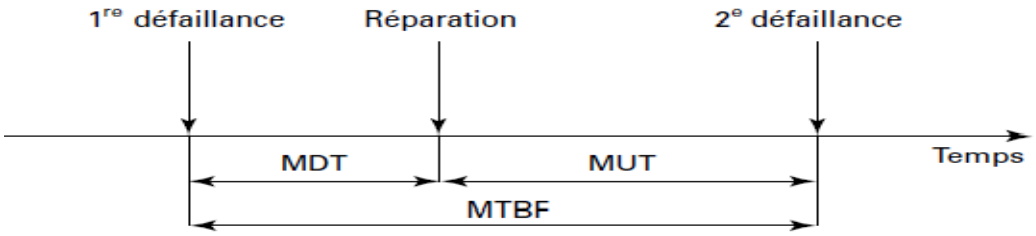


Figure1.9 Représentation des MTBF, MDT et MUT.

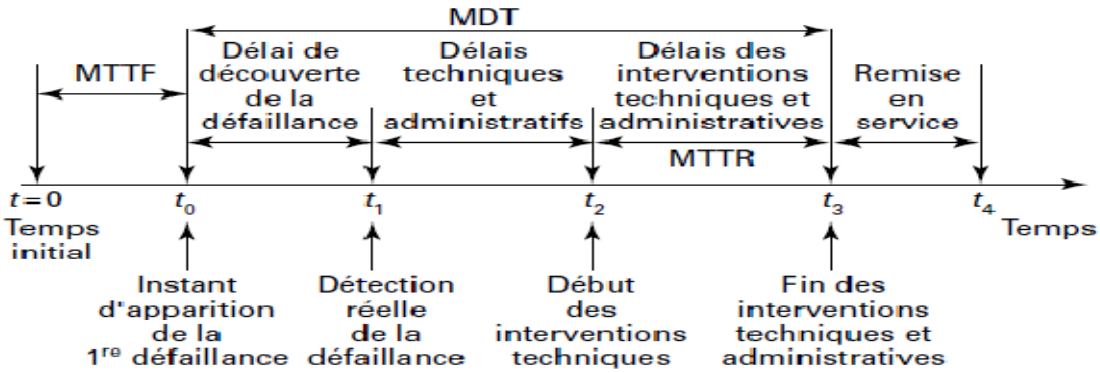


Figure 1.10 Chaînage temporel des activités de détection et de remise en service.

I.7.3.1. Les sortes de la disponibilité

❖ **Disponibilité intrinsèque**

Cette disponibilité est évaluée en prenant en compte les moyennes des temps de bon fonctionnement et les moyennes des temps de réparation.

$$D_i = \frac{MTBF}{MTBF+MTTR}$$

❖ **Disponibilité instantanée**

C'est la probabilité pour qu'un dispositif puisse accomplir une fonction requise dans des conditions données et une instante donnée[12].

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

Avec :

μ : Taux de réparation. λ : Taux de défaillance.

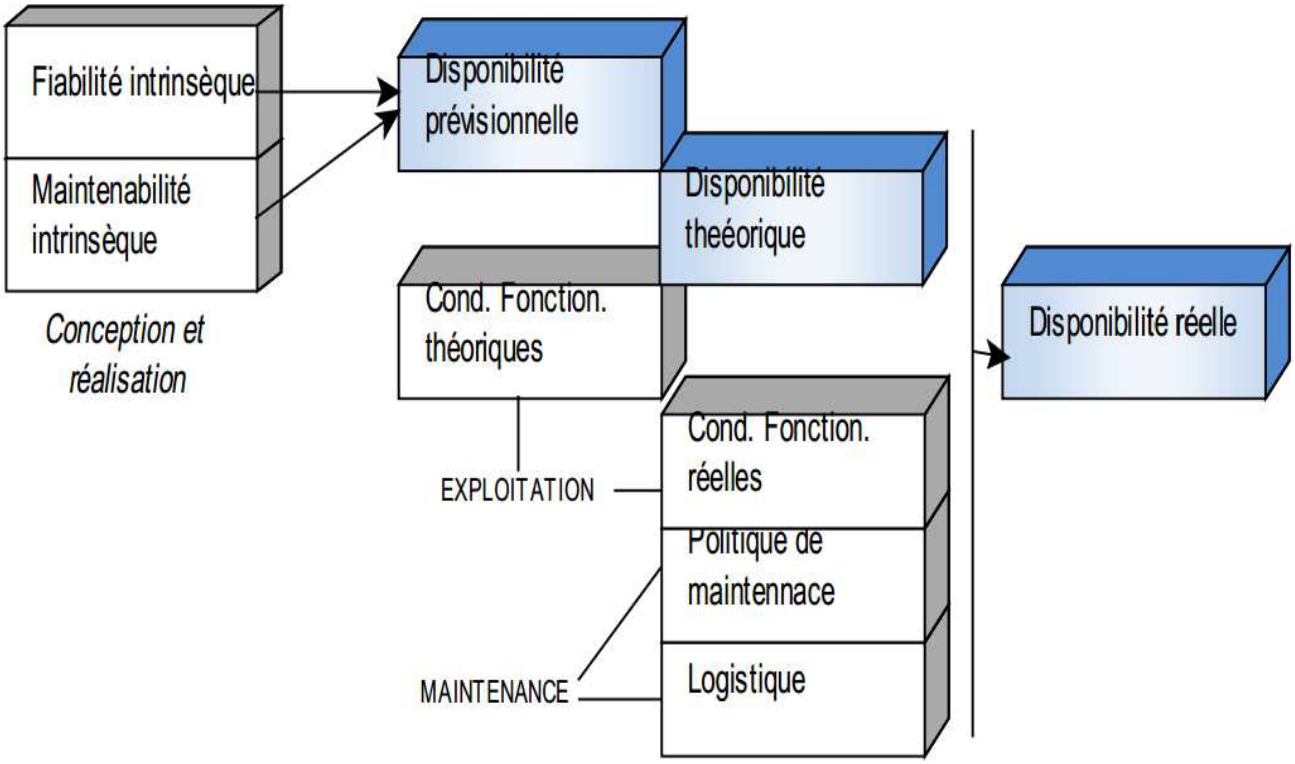


Figure I.11 : Les trois types de disponibilité.

I.7.4. La sécurité

Bien que la norme [CEI 50 (191), 1990] n'intègre pas la sécurité comme composant de la sûreté de fonctionnement, nous considérons qu'il est important de la prendre en compte car l'occurrence d'un événement catastrophique met en péril la vie humaine.

En fait, le concept de sécurité est probablement le plus difficile à définir et à évaluer, car il englobe des aspects très divers. Cependant, la norme [EN 292 – 1, 1991] sur la sécurité des machines donne cette définition :

Aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue, démontée et mise au rebut dans les conditions d'utilisation normales spécifiées dans la notice d'instructions, sans causer de lésions ou d'atteinte à la santé.

La sécurité peut également s'exprimer sous forme d'une probabilité que le système évite de faire apparaître, dans des conditions données, des événements critiques ou cata strophiques (Villemeur, 1988). Si on considère que les défaillances d'un système se partagent en deux catégories, celles qui sont dangereuses et celles qui ne le sont pas, la sécurité peut être considérée comme la part de la fiabilité relative aux défaillances dangereuses. Ce concept peut devenir prépondérant dans une analyse de sûreté de fonctionnement, dans la mesure où une défaillance du système peut présenter un risque de dommage corporel à l'encontre des usagers.

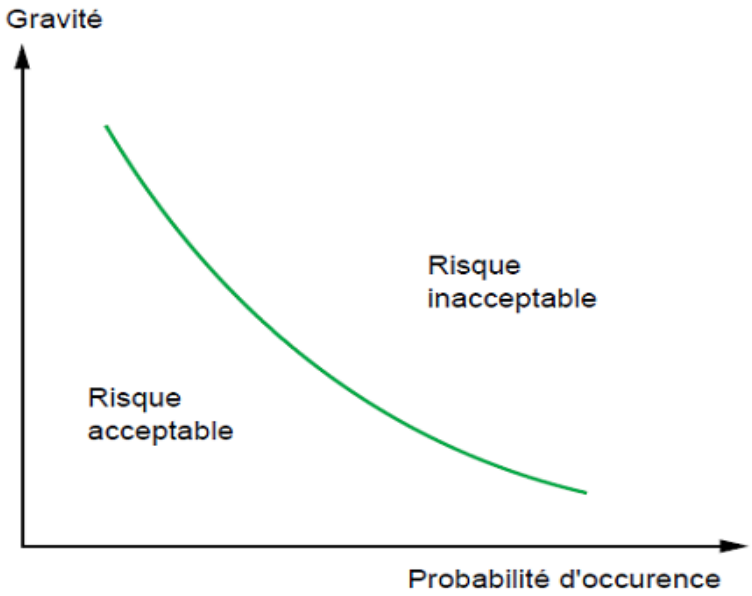


Figure I.12 : Le niveau de risque est fonction du couple : gravité, probabilité d'occurrence.

1.7.5. Etudes de sûreté de fonctionnement

Les études de sûreté de fonctionnement regroupent les activités d'évaluation prévisionnelle de la fiabilité, de la maintenabilité, de la disponibilité et de la sécurité d'une organisation, d'un système, d'un produit ou d'un moyen. Ces évaluations permettent, par comparaison aux objectifs ou dans l'absolu, d'identifier les actions de conception ou d'amélioration de l'entité pour atteindre le niveau voulu.

Ces études consistent généralement à analyser les effets des pannes, dysfonctionnements, erreurs d'utilisation ou agressions de l'entité étudiée. L'étude de sûreté de fonctionnement comporte deux volets complémentaires :

Analyse fonctionnelle va détailler la manière dont le système va opérer dans toutes ses phases de vie ainsi que les autres systèmes avec lesquels il va pouvoir interagir, Analyse dysfonctionnelle vise à imaginer l'ensemble des défaillances pouvant survenir n'importe où dans le système, seules ou combinées entre elles, et à analyser leur impact. Les résultats de ces deux études sont mis en commun dans une modélisation du système qui va représenter virtuellement celui-ci avant sa réalisation, tant dans son fonctionnement attendu que dans les pannes susceptibles de lui arriver. En étudiant cette modélisation, il devient alors possible de valider ou invalider une

solution technique, optimiser des choix architecturaux, remplacer des composants critiques, ceci dans le but de : réduire au maximum les risques ; réduire au maximum les coûts d'exploitation ; tolérer, dans la mesure du possible, certaines fautes en autorisant un fonctionnement en mode dégradé sous certaines conditions.

I.9.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 :

- ✓ des défaillances et des pannes des composants du système,
- ✓ des événements lies a l'environnement,
- ✓ 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.
An d'aider l'analyste, plusieurs méthodes d'analyse ont été mises au point. Les principales sont :

1. Analyse fonctionnelle externe (AFE)

L'analyse fonctionnelle externe (ou analyse fonctionnelle du besoin) est un outil qui décrit de façon exhaustive les fonctions à réaliser pour satisfaire les besoins réels de l'utilisateur.
Son principe est de considérer l'objet de l'étude comme une boîte noire, et de le placer dans son environnement d'utilisation pour décrire ce qu'il doit faire, faisant abstraction des solutions.

Cette approche se déroule en 7 phases :

Phase 1 : Définir les limites du système

Phase 2 : Valider le besoin du système

Phase 3 : Rechercher les situations de vie

Phase 4 : Lister les environnants au système par situation de vie

Phase 5 : Rechercher les relations entre le système et ses environnants (les fonctions)
Phase 6 : Libeller ces fonctions

Phase 7 : Caractériser ces fonctions.

2. Analyse fonctionnelle interne (AFI)

L'objet de cette analyse est de décrire comment les composants du système participent à la réalisation des fonctions. Evidemment, à ce stade, il faut avoir défini le nombre de composants et le mode de fonctionnement du système.

Cette analyse comporte deux étapes principales : la décomposition du système et l'identification des flux à l'intérieur du système.

Décomposition du système

L'objet de cette décomposition est de définir les éléments constitutifs qui composent le système. Cette décomposition va constituer la nomenclature produit.

Identification des flux à l'intérieur du système

L'objet de cette étude est de déterminer comment chaque fonction définie lors de l'analyse fonctionnelle externe, est réalisée par les différents composants. En intégrant les composants dans la bulle centrale de la pieuvre, on illustre le chemin suivi par chacune des fonctions. Ce chemin représente les flux à l'intérieur du système, flux qui sont de trois types : matière, énergie ou information. Les fonctions sont alors matérialisées dans le dessin par des traits représentant les contacts entre les éléments eux-mêmes et entre les éléments et les différents environnants. Ce schéma est classiquement appelé « bloc diagramme fonctionnel ».

3. Analyse Préliminaire des Risques (APR)

L'analyse préliminaire de risques est une méthode visant à fournir l'ensemble des événements redoutés prévisionnels dans toutes les phases de vie du système étudié. Cette analyse se décompose en deux approches complémentaires :

une approche fonctionnelle : analyse des conséquences des défaillances des fonctions du système, une approche agressions : analyse des conséquences des agressions du système vers l'extérieur (éléments potentiellement dangereux) ; analyse des conséquences des agressions du milieu extérieur vers le système (éléments sensibles).

Ces approches ont pour avantages d'obtenir un examen rapide des situations dangereuses, ne

nécessitant pas un niveau de description détaillé du système étudié. Par contre, pour des systèmes complexes, elles ne permettent pas de décrire finement les enchaînements qui conduisent à une défaillance majeure : l'utilisation ultérieure d'outils tels que l'AMDEC ou arbre de défaillances sont nécessaires.

L'approche fonctionnelle a pour but d'étudier les conséquences de chaque mode de défaillance des fonctions décrites dans l'analyse fonctionnelle. Elle est donc effectuée pour chaque fonction du système dans chaque situation de vie. Par mode de défaillance, on entend :

Absence de fonction à la sollicitation: ça ne marche pas,
Perte de fonction en fonctionnement : ça ne marche plus,
Fonctionnement dégradé : ça marche mal,

Fonctionnement intempestif : ça marche alors que l'on a rien demandé,

Fonctionnement intermittent : ça s'arrête et ça repart tout seul.

Toutes les fonctions de service et les fonctions contraintes listées dans l'analyse fonctionnelle externe sont reprises comme données d'entrée pour l'APR approche fonctionnelle. Pour chaque fonction, les modes de défaillance seront déterminés en tenant compte des différents types définis ci-avant (absence, perte, dégradé, intempestif et intermittent). Ensuite, l'événement redouté par le client est identifié pour chaque mode de défaillance. Par client, on entend l'utilisateur final du macro-système dans la situation de vie étudiée. L'événement redouté s'exprime donc en termes de gêne pour le client, allant de l'insatisfaction jusqu'à l'atteinte de l'intégrité physique de l'utilisateur ou des personnes environnantes.

4. Arbre de défaillances (ADD)

4.1 Construction de l'arbre de défaillances

L'arbre de défaillances est un outil déductif et itératif : on part d'un effet pour en trouver ses causes en se posant la question « Pourquoi ? ». A la différence du diagramme « Causes – Effets » ou de l'outil « 5 Pourquoi ? » où chaque cause peut individuellement entraîner l'effet non désiré, l'arbre de défaillances permet, en plus, de mettre en évidence la combinatoire de ces causes. Même si classiquement, un arbre de défaillances est représenté verticalement, on conviendra d'une représentation de l'arbre couché où l'événement redouté est à gauche et les causes s'enchaînent vers la droite.

Définition de l'événement redouté (« sommet de l'arbre »)

L'événement redouté (ER) est l'événement indésirable pour lequel on recherche toutes les causes, et leur combinatoire, qui y conduisent. Cet événement est unique pour un arbre de défaillances et se trouve à gauche de l'arbre (ou au sommet). Il doit être défini de façon précise afin d'éviter d'avoir une analyse gigantesque ou impossible à faire. Cet événement provient généralement de l'analyse préliminaire de risques utilisée en amont de l'arbre de défaillances.

Portes logiques

L'arbre de défaillances est particulièrement bien adapté aux événements combinatoires, mais devient délicat à mettre en œuvre quand il s'agit d'événements séquentiels.

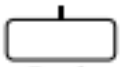
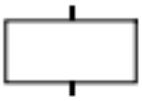
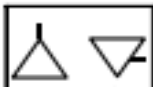
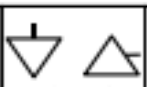
L'analyse débute par la recherche des causes immédiates nécessaires et suffisantes pour obtenir l'événement redouté. Ces causes constituent des événements intermédiaires dont on recherchera les causes et leur combinatoire, et ainsi de suite. A chaque étape, la question pertinente pour rechercher les causes du niveau inférieure est « pourquoi ? ».

Les causes correspondant au niveau le plus à droite (ou plus bas) de l'analyse sont appelées événements élémentaires ou causes racines. Ces causes racines seront identifiées d'une couleur spécifique dans l'arbre (la couleur jaune sera préconisée).

La difficulté de l'arbre de défaillances est de définir le niveau de détail adapté. De façon générale, nous considérons que les événements élémentaires correspondent aux défaillances des composants, un composant étant un sous-système réparable ou interchangeable.

Dans le cas d'un arbre de défaillances mis en œuvre dans le cadre d'une démarche Sureté de Fonctionnement, les événements de base correspondent aux défaillances des sous-systèmes de niveau N-1 définis dans notre décomposition hiérarchique du produit appelée découpage PBS (Product Breakdown Structure).

Dans la réalisation de l'arbre, le groupe de travail veillera à bien rester dans ses limites de responsabilité tout en communiquant les causes identifiées à d'autres intervenants : client, fournisseur...

 Cercle	Evt élémentaire ne nécessitant pas de développement futur	 Ovale	Evt conditionnel qui peut être utilisé avec certaines portes logiques
 Losange	Evt qui ne peut être considéré comme élémentaire, mais dont les causes ne sont et ne seront pas développées	 Double losange	Evt dont les causes ne sont ne sont pas développées mais le seront ultérieurement
 Rectangle	Résulte de la combinaison d'autres évts par l'intermédiaire d'une porte logique	 Maison	Evt qui correspond à un fct. normal du $\sum$ (P=1)
 Triangle	La partie de l'arbre qui suit le 2ème symbole est transférée à l'emplacement du 1er	 Triangle inversé	Une partie semblable, mais non identique à celle qui suit le 2ème symbole est transférée à l'emplac[1] du 1er

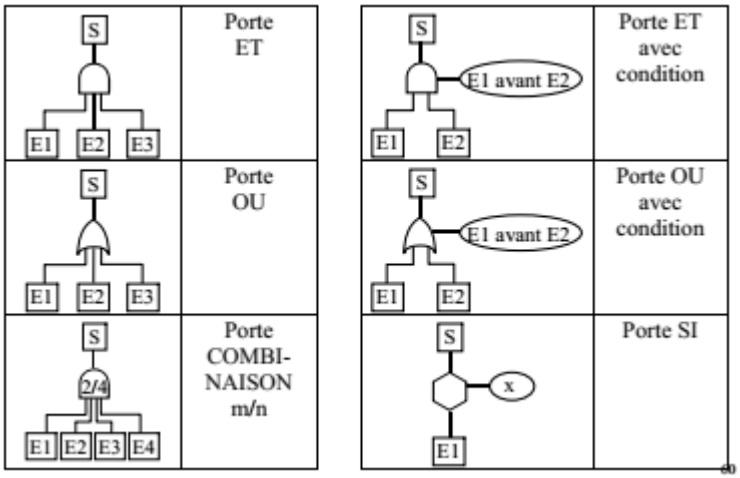
Une des utilisations de l'arbre des défaillances est l'allocation des objectifs de fiabilité à chacun des composants du système par une quantification de type « Top Down » : en partant de l'objectif alloué au système complet (gauche de l'arbre), on donne un objectif de fiabilité à chacune des causes élémentaires (racines de l'arbre). Ainsi, conformément à l'algèbre de Boole :

Probabilité (A et B) = P (A) x P (B)

Probabilité (A ou B) = P (A) + P (B) - P (A) x P (B) = P (A) + P (B)- P (A) x P (B)

P (A) x P (B) est négligeable étant donné que les probabilités P (A) et P (B) sont faibles. Par conséquent, à chaque passage de ET, on prend la racine carré de l'objectif de l'événement supérieur (à gauche) ou on divise cet objectif en traversant un OU. Une répartition peut également être effectuée au prorata des retours observés sur les systèmes de génération précédente.

Cette approche peut donc permettre d'objectiver les valeurs des objectifs de fiabilité alloués aux fournisseurs de sous-systèmes.

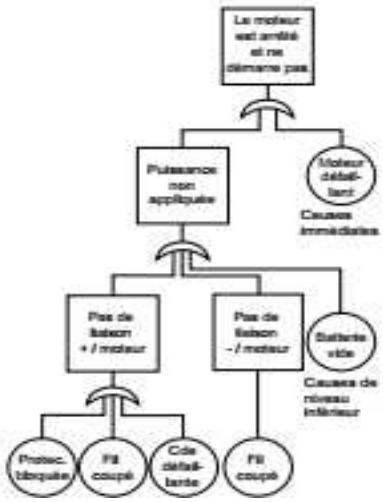


Exemple:

L'arbre de défaillance de la figure ci-contre avec l'évènement redouté:

"Le moteur ne marche pas".

Schéma d'alimentation d'un moteur électrique



5Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC)

L'AMDEC est définie comme étant une méthode rigoureuse et préventive visant à recenser puis à évalue les défaillances d'un système.

Cette méthode est considérée par la plupart des industriels comme l'outil d'analyse de risque le plus pertinent.

5.1AMDEC Produit

L'AMDEC Produit est utilisée pour fiabiliser les systèmes par l'analyse des défaillances dues aux erreurs de conception. Ce type d'AMDEC est donc initialisé en phase de développement produit au moment de sa conception.

Elle a pour objet de s'assurer que le « Design » répond à l'ensemble des critères du cahier des charges : les modes de défaillance seront considérés comme étant la non-réalisation ou la mauvaise réalisation des critères de performance associés aux fonctions décrites dans l'analyse fonctionnelle du produit.

Cette analyse se décompose en trois parties :

Analyse qualitative : à partir des fonctions du produit, identification des modes de défaillance potentiels, de leurs effets, de leurs causes, des contrôles de conception existants (prévention et détection),

Analyse quantitative : évaluation du risque lié à chaque mode de défaillance (gravité, occurrence, détection IPR),
Plan d'actions correctives pour réduire les niveaux de risque les plus élevés : actions au niveau de la conception du produit et actions pour améliorer les démarches de validation prévues.

5.2AMDEC Process

L'AMDEC Process est utilisée pour analyser les défaillances générées par le processus de fabrication. Ce type d'AMDEC est idéalement initialisé en phase d'industrialisation au moment de la définition du processus de fabrication et de la conception des moyens.

Elle a pour objet de s'assurer que le processus de fabrication répond à l'ensemble des exigences définies pour la réalisation des opérations : les modes de défaillance seront considérés comme étant la non-réalisation ou la mauvaise réalisation des exigences produit/process associées aux opérations décrites dans la décomposition fonctionnelle du processus de fabrication (incluant la réception, les flux inter-postes, les contrôles et la livraison). Cette analyse se décompose en trois parties :

Analyse qualitative : à partir des opérations élémentaires de fabrication, identification des modes de défaillance potentiels, de leurs effets, de leurs causes, des contrôles de processus existants (prévention et détection),

Analyse quantitative : évaluation du risque lié à chaque mode de défaillance (gravité, occurrence, détection IPR),

Plan d'actions correctives pour réduire les niveaux de risque les plus élevés : actions au niveau de la conception du produit/process et actions pour améliorer les détections prévues (contrôles).

Le tableau ci-après reprend le formalisme standard utilisé pour les AMDEC Process, quelque soit l'exigence du client.

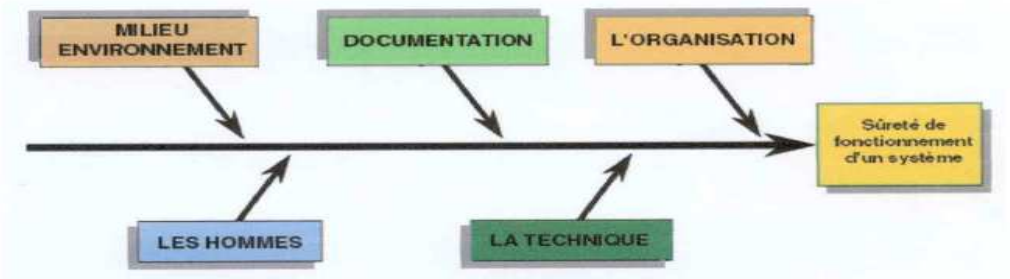
Elément	Fonction	Mode	Cause	Effet	Evaluation	Détection	Action

Le mode de défaillance

Il concerne la fonction et exprime de quelle manière cette fonction ne fait plus ce qu'elle est sensée faire. L'analyse fonctionnelle recense les fonctions, l'AMDEC envisage pour chacune d'entre-elles sa façon (ou ses façons car il peut y en avoir plusieurs) de ne plus se comporter correctement.

La cause

C'est l'anomalie qui conduit au mode de défaillance. La défaillance est un écart par rapport à la norme de fonctionnement. Les causes trouvent leurs sources dans cinq grandes familles. On en fait l'inventaire dans des diagrammes dits "diagrammes de causes à effets"



Un mode de défaillance peut résulter de la combinaison de plusieurs causes.

Une cause peut être à l'origine de plusieurs modes de défaillances.

L'effet

L'effet concrétise la conséquence du mode de défaillance. Il dépend du point de vue AMDEC que l'on adopte :

• effets sur la qualité du produit (AMDEC procédé)

• effets sur la productivité (AMDEC machine)

• effets sur la sécurité (AMDEC sécurité)

Un effet peut lui-même devenir la cause d'un autre mode de défaillance

L'évaluation

L'évaluation se fait selon 3 critères principaux :

• la gravité

• la fréquence

• la non-détection

Ces critères ne sont pas limitatifs, le groupe de travail peut en définir d'autres plus judicieux par rapport au problème traité.

Chaque critère est évalué dans une plage de notes.

Cette plage est déterminée par le groupe de travail.

exemple :	de 1 à 4 de 1 à 10

Plus la note est élevée, plus sa sévérité est grande.

Une plage d'évaluation large oblige à plus de finesse dans l'analyse, ce qui peut donner lieu à des controverses au sein du groupe.

Le nombre de niveaux d'évaluation doit être pair pour éviter le compromis moyen systématique sur une note centrale (exemple : éviter les plages telles que 1 à 5 car la note 3 aura tendance à être adoptée trop souvent au titre du compromis).

La gravité

Elle exprime l'importance de l'effet sur la qualité du produit (AMDEC procédé) ou sur la productivité (AMDEC machine) ou sur la sécurité (AMDEC sécurité).

Le groupe doit décider de la manière de mesurer l'effet.

Exemple :
effet sur la dimension d'un produit : effet sur le temps d'arrêt de production

note 1 :	écart inférieur à 0,5%
note 2 :	écart inférieur à 1%
note 3 :	écart inférieur à 5%
note 4 :	écart supérieur à 5%

note 1 :	inférieur à 4 heures
note 2 :	inférieur à 24 heures
note 3 :	inférieur à 1 semaine
note 4 :	supérieur à une semaine

La fréquence

On estime la période à laquelle la défaillance est susceptible de se reproduire

exemple :

note 1 :	moins d'une fois par an
note 2 :	moins d'une fois par mois
note 3 :	moins d'une fois par semaine
note 4 :	plus d'une fois par semaine

La non-détection

Elle exprime l'efficacité du système permettant de détecter le problème

exemple :

note 1 :	détection efficace permettant une action préventive
note 2 :	système présentant des risques de non-détection dans certains cas
note 3 :	système de détection peu fiable
note 4 :	aucune détection

La criticité

Lorsque les 3 critères ont été évalués dans une ligne de la synthèse AMDEC, on fait le produit

des 3 notes obtenues pour calculer la criticité.

C = G * F * N

criticité =gravité *fréquence* non-détection

Le groupe de travail doit alors décider **d'un seuil de criticité.**

Au delà de ce seuil, l'effet de la défaillance n'est pas supportable. Une action est nécessaire.

Les actions

La finalité de l'analyse AMDEC, après la mise en évidence des défaillances critiques, est de définir des actions de nature à traiter le problème identifié.

Les actions sont de 3 types :

Actions préventives : on agit pour prévenir la défaillance avant qu'elle ne se produise, pour l'empêcher de se produire. Ces actions sont planifiées. La période d'application d'une action résulte de l'évaluation de la fréquence.

Actions correctives : lorsque le problème n'est pas considéré comme critique, on agit au moment où il se présente. L'action doit alors être la plus courte possible pour une remise aux normes rapide.

Actions améliorative : il s'agit en général de modifications de procédé ou de modifications technologiques du moyen de production destinées à faire disparaître totalement le problème. Le coût de ce type d'action n'est pas négligeable et on le traite comme un investissement

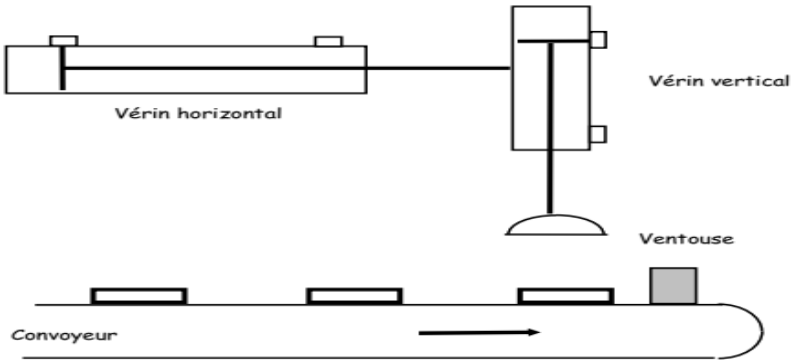
.

Les actions, pour être efficaces, doivent faire l'objet d'un suivi :

- plan d'action
- désignation d'un responsable de l'action
- détermination d'un délai
- détermination d'un budget
- révision de l'évaluation après mise en place de l'action et retours des résultats.

Exemple d'application;

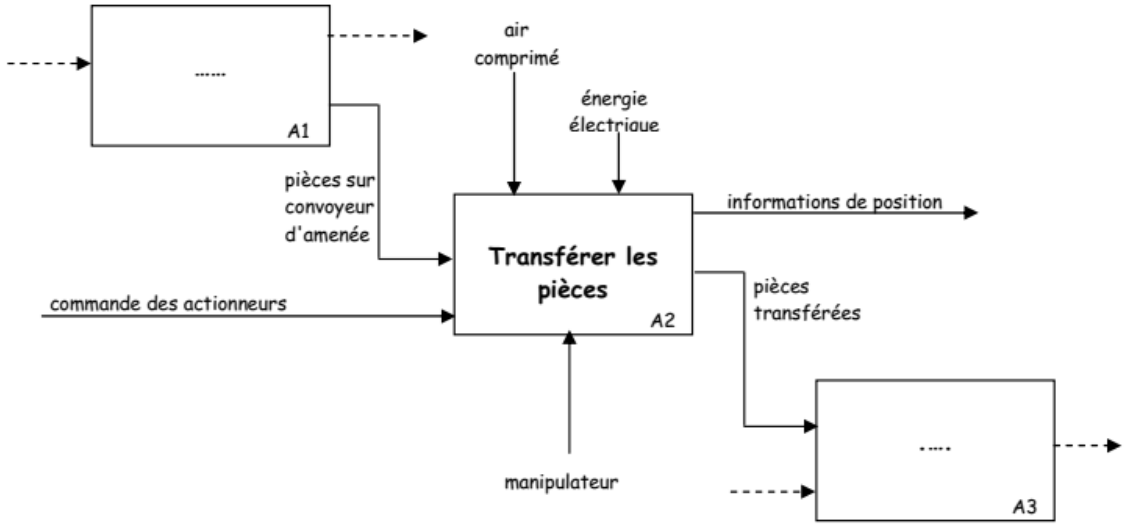
On considère une fonction de transfert de pièces réalisée par un manipulateur pneumatique. Cette fonction est elle-même intégrée dans une fonction de production.



‹

Analyse fonctionnelle descendante

niveau 0



La fonction A2 "Transférer les pièces" peut elle-même être décomposée en sous fonctions.

Analyse structurelle

La référence à un dossier technique (électrique, pneumatique, mécanique) est nécessaire.

Manipulateur	Unité verticale	Distributeur électropneumatique de montée Tubes Vérin Limiteurs de débit Capteur vérin haut Capteur vérin bas
	(la commande de ce vérin est monostable)	
	Unité horizontale	Distributeur électropneumatique de sortie Distributeur électropneumatique de rentrée Tubes Vérin Limiteurs de débit Capteur vérin rentré Capteur vérin sorti
	(la commande de ce vérin est bistable)	
	Aspiration	Distributeur électropneumatique d'aspiration Tubes Venturi Ventouse
	(l'aspiration n'est pas contrôlée)	

Définition des critères

Les critères ci-après répondent à une AMDEC de type machine orientée maintenanc

La gravité

note 1 : arrêt production inférieur à 1 heure
note 2 : arrêt production inférieur à 4 heures
note 3 : arrêt production inférieur à 1 jour
note 4 : arrêt production supérieur à 1 jour

La fréquence

note 1 : moins d'une fois par an
note 2 : moins d'une fois par mois
note 3 : moins d'une fois par semaine
note 4 : plus d'une fois par semaine

La non-détection

note 1 : détection efficace permettant une action préventive
note 2 : système présentant des risques de non-détection dans certains cas
note 3 : système de détection peu fiable
note 4 : aucune détection

La criticité

$$C = G * F * N$$

Le seuil de criticité est fixé à 8

Fonction	Matériel ou sous-ensemble	Mode de défaillance	Cause	Effet	G	F	D	C	Détection	Action
Transférer les pièces	Distributeurs électropneumatiques	Le distributeur ne bascule pas quand il est commandé	Bobine grillée	Cycle bloqué	1	2	3	6	Alarme automate	
			Mauvaise connexion		1	1	3	6	Alarme automate	
			Tiroir bloqué		1	1	3	3	Alarme automate	
	Tubes	L'air passe mal	Rupture ou pliure	Cycle ralenti	1	1	4	4	Visuel	
	Vérins (vertical et horizontal)	Le vérin ne bouge pas ou très lentement	Vérin grippé	Cycle ralenti	2	2	4	16	Visuel	Contrôle périodique
			Vérin usé (perte d'étanchéité)		2	2	4	16	Visuel	Contrôle périodique
	Limiteurs de débit	L'air passe mal	Limiteur bouché ou mal réglé	Cycle ralenti	1	1	4	4	Visuel	
		Le débit n'est pas réduit	Mal réglé	Course du vérin trop rapide	1	1	4	4	Visuel	
	Capteurs	Non détection de la position	Mauvais réglage	Cycle bloqué Marche dégradée	1	3	2	6	Alarme automate	
			Capteur grillé		1	3	2	6	Alarme automate	
			Mauvaise connexion		1	1	2	2	Alarme automate	
		Détection permanente	Capteur en court-circuit	Cycle désordonné	3	2	4	24	Visuel	Contrôle par automate
	Ventouse	Pas d'aspiration	Vent. bouchée	Pas de transfert	1	3	4	12	Visuel	Contrôle
			Vent. usée	Pas de transfert	1	1	4	4	Visuel	
	Venturi	Pas d'aspiration	Encrassement	Pas de transfert	1	2	4	8	Visuel	périodique