République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département de Génie Electrotechnique et Automatique

Mémoire de fin d'étude
Pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Techniques**
Filière : **Automatique et informatique industrielle**
Spécialité : **Commande et diagnostic des systèmes industriels**

Recherche des scenarios critiques par la méthode des arbres de défaillance

---

Présenté par : **Zerguine AMMAR**

Sous la direction de : **Boucceradj LAILA**

JUIN 2011

TABLE DE MATIERE

Chapitre 2 « Méthode d'analyse de la Sureté de Fonctionnement »

Chapitre 3 « Application au système de régulation des réservoirs

Dédicaces

A mon père, merci papa pour tes encouragements et ton soutien moral et ma mère.

A mes sœurs et mes frères
A toute ma famille.
A tous mes amis et mes collègues.
A mon encadreuse boucceradj laila pour son aide.

Remerciement

Mes premiers remerciements s'adressent à mon encadreuse boucceradj laila pour l'intérêt qu'elle porte au développement de la recherche en me proposant ce sujet: « recherche des scénarios critiques par la méthode des arbres de défaillance »

Sa culture scientifique, son exigence, sa persévérance, et sa rigueur, ont été plus que bienvenus : ils ont été indispensables pour mener à bien cette aventure et pour diriger mes travaux. Je suis encore une fois reconnaissant pour m'avoir permis l'accès libre à sa documentation personnelle.

J'exprime toute ma gratitude pour les membres de juré pour m'avoir fait le très grand honneur d'examiner mes travaux de master .

Un grand merci a toute l'équipe du Génie Electrotechnique et Automatique dans son ensemble .

Merci à ma famille pour son amour, à mes amis pour leur soutien et leur présence. ..et tous ceux qui m'ont vraiment aidés.

Introduction générale

Les progrès scientifiques et technologiques ont grandement contribué à la réalisation des systèmes industriels compétitifs. En générale, ces systèmes sont devenus complexes, et il est difficile d'évaluer leur comportement lorsqu'ils sont le siège de perturbation. De nombreux exemples, tel l'accident de *SONATRACH* de *SKIKDA*, ont montré que ces perturbations pouvaient mener le système dans un état défaillant, non sécuritaire et avoir un impact non négligeable sur certains enjeux socio-économiques essentiellement liés : à la sécurité des hommes et des matériels, à la protection de l'environnement et aux gains de productivité.

Les prévisions et les préventions de tels événements sont l'objet de préoccupation non seulement de la part des industriels, quel que soit leur domaine (aéronautique, transport, etc...) mais également des ministères publics. Dans ce contexte, l'évaluation de la sûreté de fonctionnement se révèle cruciale pour maîtriser les risques induits par la défaillance d'un système et elle est devenue un critère de référence pour leur mise en service. L'évaluation de la sûreté se concentre plus exactement sur la compréhension du fonctionnement et du dysfonctionnement du système.

La complexité des systèmes mécatroniques rend difficile la maîtrise de leur fiabilité. Ces systèmes alliant mécanique, hydraulique, électronique, et logiciels sont hybrides : la dynamique continue est associée à la partie énergétique et la dynamique discrète est liée à la commande numérique et à l'existence d'événements discrets (défaillances, dépassements de seuils) [1].

C'est à partir de ce constat que nous avons entrepris cette étude, donc ce travail s'intéresse à la sécurité des systèmes mécatroniques. Dont l'objectif est de caractériser les scénarios redoutés au plus tôt dans la phase de conception des systèmes.
Une analyse qualitative et quantitative de ces scénarios est nécessaire pour choisir les architectures les plus sûres.

Nous avons choisi la méthode des arbres de défaillances basée sur l'analyse qualitative et quantitative permettant de déduire les scénarios redoutés, en particulier en déterminant la suite d'actions et d'états conduisant à l'état redouté.

Ce mémoire est structuré en trois chapitres, dans le premier chapitre nous introduirons quelques notions relatives à la conception de la sûreté de fonctionnement. Les principales méthodes liées à l'évaluation des paramètres Fiabilité Maintenabilité Disponibilité Sécurité (FMDS).
Le deuxième chapitre présente les méthodes d'analyse de la sûreté de fonctionnement.
Enfin le dernier chapitre portera sur l'application de la méthode des arbres de défaillance elle est basée sur la recherche de cause à effet pour un système de régulation de deux réservoirs.

Et finalement, une conclusion générale dans laquelle on présente les perspectives offertes par ce travail.

Chapitre 1
Sûreté de Fonctionnement

I.1 Introduction

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

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

I.2 L'importance de la sûreté

L'homme des cavernes devait être sûr de son bras. L'homme moderne est entouré d'outils, de systèmes de plus en plus sophistiqués dont il doit être sûr, ceci s'il veut qu'ils concourent réellement à sa sécurité, son efficacité et son confort [1].

I.2.1 Dans le logement

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

- La fiabilité de son téléviseur.
- La disponibilité de l'électricité.

- La réparabilité de son congélateur ou de sa voiture.
- La sécurité du coupe-gaz de sa chaudière [1].

I.2.2 Dans le tertiaire

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

- La fiabilité de l'informatique.
- La disponibilité du chauffage.
- La réparabilité des ascenseurs.
- La sécurité incendie.

I.2.3 Dans l'industrie

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

- Fiabilité de ses systèmes contrôle commande.
- Disponibilité de ses machines.
- Maintenabilité de l'outil de production.
- Sécurité des personnes et du capital industriel.

Ces valeurs que l'on regroupe sous le concept de SURETE (être sûr) font appel à la notion de confiance. Elles se quantifient en terme d'objectif, se calculent en terme de probabilité, se réalisent en terme d'architecture et de choix de composants, se vérifient par les tests ou l'expérience [1].

1.3 Définition de la sûreté de fonctionnement

La sûreté de fonctionnement noté (SDF: Dependability) peut être définit, au sens large, comme la science des défaillances qui inclut leur connaissance, leur évaluation, leur prévision leur prévision leur mesures et leur maîtrise, ceci dans un double but: d'une part atteindre les objectifs pour lesquels le système est réaliser (performance, durée de vie,...), d'autre part respecter la sécurité du système et de son environnement(destruction matérielles, agression humain...) dans un souci permanant d'optimisation des coûts.

Au sens strict, la sûreté de fonctionnement permet d'établir le degré de confiance que l'on peut attribuer à un système danse cadre de sa mission qu'il doit assurer. Ce degré de confiance est donné par les concepts suivants, la sûreté de fonctionnement regroupe des

modèle, des méthodes, des outils et des compétences permettant la maîtrise de critères tels que la fiabilité, la maintenabilité, la sécurité, la disponibilité, la confidentialité, etc... D'un système. Les trois premiers critères ont été considérés comme les plus significatifs vis-à-vis du système industriel et ils sont détaillés à présent.

I.4 Notions de temps

L'étude de la SdF est liée aux temps moyens suivants :

MTTF signifie "Mean Time To Failure" (Temps moyen de fonctionnement avant panne).

MTBF signifie "Mean Time Between Failure" (Temps moyen entre pannes).

Les anglo-saxons définissent aussi le :

MUT "Mean Up Time" (temps moyen de disponibilité), le système n'est pas nécessairement entièrement réparé s'il y a redondance.

MDT "Mean Down Time" (durée moyenne d'indisponibilité), qui comprend la détection, la réparation de la panne et la remise en service.

MTTR signifie "Mean Time To Repair" (Durée moyenne de réparation).

On a la relation, MTBF = MDT + MUT pour les systèmes redondants (défaillance ≠panne)
(Dans certains cas, nous avons MDT = MTTR (Mean Time To Repair).
Pour de nombreux systèmes, MDT est faible devant MUT, et donc la différence entre MTTF et MTBF est faible.

I.5 Concept de fiabilité des systèmes

I.5.1 Définitions

La fiabilité (R - *Reliability*) est l'aptitude (la probabilité) d'une entité à accomplir une fonction requise pendant un intervalle de temps donné, dans des conditions données.
L'entité peut être un composant, un système, un réseau ou même un logiciel. La fonction requise, nécessaire pour la fourniture d'un service donné, doit être spécifiée dans un cahier des charges avec les tolérances acceptables. Les conditions d'emploi sont liées à l'environnement climatique, mécanique, chimique ou électrique.
C'est le maintien de la qualité dans le temps, sans discontinuité. Le temps est donc la variable principale mais il peut être parfois remplacé par une autre : nombre de cycles d'ouverture/fermeture pour un relai, d'accouplements pour un connecteur, nombre de tours

pour un moteur... (Exception : les fusibles dont l'utilisation entraîne la destruction). C'est une fonction décroissante comprise entre 1 et 0.

Aptitude d'un bien à accomplir une fonction requise dans des conditions données pendant un temps donné ou "caractéristique d'un bien exprimée par la probabilité qu'il accomplisse une fonction requise dans des conditions données pendant un temps donné".

La notion de temps peut prendre la forme :

- De nombre de cycles effectués machine automatique.
- De distance parcourue matériel roulant.
- De tonnage produit équipement de production.

La fiabilité est la probabilité pour qu'un appareil fonctionne sans défaillance pendant une durée de temps. Durée de vie ou temps de bon fonctionnement d'un appareil C'est la variable aléatoire T qui à tout appareil associe sa durée de vie ou le temps de bon fonctionnement d'un appareil, c'est à dire l'instant ou apparaît la première défaillance (en général, on choisit $t = 0$ comme instant de mise en service de l'appareil)[5] .

Un équipement est fiable s'il subit peu d'arrêts pour pannes. La notion de fiabilité s'applique

- A du système réparable $\Rightarrow$ équipement industriel ou domestique.
- A des systèmes non réparables $\Rightarrow$ lampes, composants donc jetables.

La fiabilité d'un équipement dépend de nombreux facteurs.

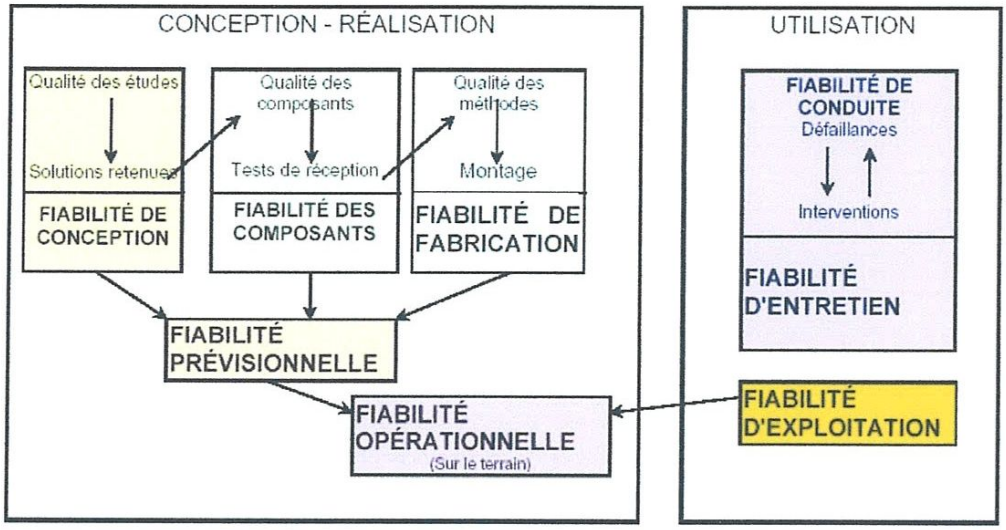


Figure I.1 : Différentes formes de fiabilité

On distingue plusieurs types de fiabilité (termes spécifiques) :

- La fiabilité opérationnelle (observée ou estimée) déduite de l'analyse d'entités identique 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 exploitation ou interpolation pour des conditions ou des durées différentes.
- La fiabilité intrinsèque ou inhérente qui découle directement des paramètres de conception sans un niveau de fiabilité au plus égal à la fiabilité intrinsèque.

I.5.2 Fonction de fiabilité et fonction de défaillance

I.5.2.1 Définition de la fonction de fiabilité

R(t) est appelée la « fonction fiabilité » (fonction mathématique du temps t, variant entre o et 1), elle est définie sur [0 ; + ∞[par :

$$R(t) = P(T \notin [0 ; t]) = P(T > t) = 1 - P(T \leq t) = 1 - F(t)$$

Où F est la fonction de répartition de la variable aléatoire T.

Remarque 1

C'est la probabilité qu'il n'y ait aucune défaillance avant t unités de temps. La fonction de répartition F de la variable aléatoire T est appelée aussi fonction de défaillance puisque c'est la probabilité d'avoir une défaillance avant l'instant t.

I.5.2.2 Estimation

On prélève un échantillon de N d'appareils et on pose

N_0 : Le nombre d'appareils n'aillant subi aucune défaillance avant l'instant t.

N_d : Le nombre d'appareils ayant subi une défaillance avant l'instant t.

N_s : Est le nombre de composantes encore en marche ou survivant à l'instant t.

On peut estimer R(t) par $N_s / N_0 = 1-N_d(t)/N_0$ et F(t) par N_d/N_0.

I.5.2.3 Densité de défaillance

Une défaillance - failure - est la cessation de l'aptitude d'une entité à accomplir une fonction requise, qui passe dans l'état de panne. La densité de défaillance f est la densité de probabilité de la variable aléatoire T définie plus haut.

On a pour tout réel t positif :

$$F'(t) = f(t)$$

où F est la fonction de répartition de la variable aléatoire T.

F est la primitive de la fonction f qui s'annule en 0.

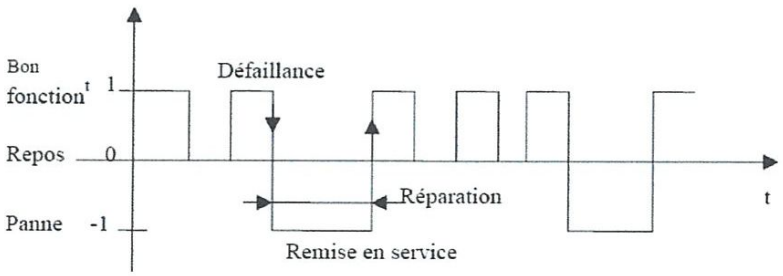


Figure I.2 : Evolution temporelle

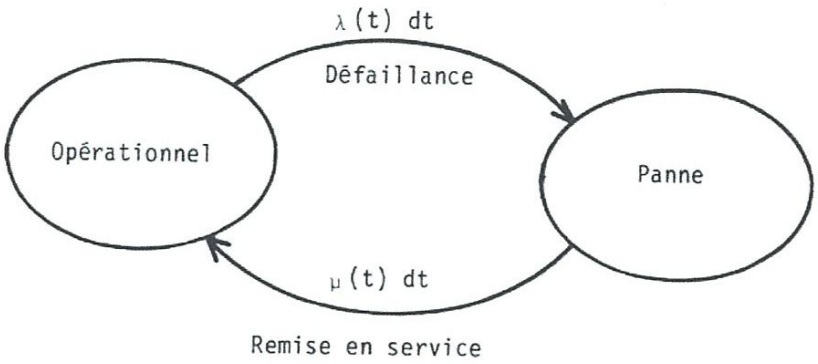


Figure I.3 : Diagramme d'état

I.5.2.4 Taux de défaillance

On appelle taux de défaillance moyen entre les instants t et $t + h$, le rapport de la probabilité qu'un appareil ait une défaillance entre les instants t et $t + h$ sachant qu'il a fonctionné avant l'instant t par h.

On appelle taux de défaillance instantané à l'instant t, la limite quand elle existe du taux de défaillance moyen entre les instants t et $t + h$ quand h tend vers 0. On note $\lambda(t)$, le taux de défaillance à l'instant t.

- ***Taux moyen***

$$\frac{P(T \in]t;t+h)] \setminus T \in]t;+\infty[)}{h} = \frac{P_{T \in]t;+\infty[}(T \in]t;t+h)])}{h}$$
$$= \frac{P(T \in]t;t+h)] et\ T \in]t;+\infty[)}{h \times P(T \in]t;+\infty[)} = \frac{P(T \in]t;t+h)])}{h \times P(T \in]t;+\infty[)}$$
$$= \frac{1}{h} \times \frac{F(t+h) - F(t)}{1 - P(T \leq t)} = \frac{1}{h} \times \frac{F(t+h) - F(t)}{1 - F(t)}$$
$$= \frac{1}{h} \times \frac{1 - R(t+h) - (1 - R(t))}{R(t)} = \frac{1}{h} \times \frac{R(t) - R(t+h)}{R(t)} \qquad (1.1)$$

- ***Taux instantanée***

$$\frac{1}{h} \times \frac{R(t) - R(t+h)}{R(t)} = \frac{-1}{R(t)} \frac{R(t+h) - R(t)}{h}$$

$$\lambda(t) = \lim_{h \to 0} \frac{-1}{R(t)} \frac{R(t+h) - R(t)}{h} = \frac{-1}{R(t)} R'(t) = \frac{-R'(t)}{R(t)}$$

$$\lambda(t) = \frac{-R'(t)}{R(t)} \qquad (1.2)$$

Le taux de défaillance ou d'avarie λ caractérise la vitesse de variation de la fiabilité au cours du temps. La durée du bon fonctionnement est égale à la durée totale en service moins la durée des défaillances.

$$\lambda = \frac{\text{Nombre total de défaillances pendant le service}}{\text{Durée totale de bon fonctionnement}} \qquad (1.3)$$

Il s'exprime en FIT Failure In Time, la durée fixée étant 10^9 heures.

I.5.2.5 Moyenne des Temps de Bon Fonctionnement

La fiabilité peut se caractériser par la Moyenne des temps de bon fonctionnement ou MTBF (Mean Time between Failure) : le temps moyen entre deux défaillances consécutives de l'appareil, c'est l'espérance mathématique de la variable aléatoire T : MTBF = E (T)
Il peut être exprimé par :

$$\text{MTBF} = \frac{\text{La somme Des temps de bon fonctionnement entre les n défaillances}}{\text{Nombre des temps de bon fonctionnement (nb défaillances)}} \qquad (1.4)$$

Remarque 2

Lorsque le taux de défaillance instantané est constant : $\lambda(t) = \lambda$= constante
MTBF=$1/\lambda$.

Exemple 1.1 *: Dans cette partie, on s'intéresse au temps de bon fonctionnement (MTBF) d'une presse. A chaque panne, on associe le nombre de jours de bon fonctionnement ayant précédé de cette panne* [5].

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 précédé la panne (en jour)	55	26	13	80	14	21	124	35	18	26

Le temps moyen de bon fonctionnement entre deux pannes exprimé en jour est :
MTBF= 55 + 26 +13+80 +14 + 21+124 + 35 +18 + 26 /11=37.4=37 jours.

I.5.3 Durée de vie utile d'un équipement

L'expérience montre que l'on peut définir trois périodes dans la vie d'un équipement sous une forme générale dite en baignoire :

- Le début de vie, qui voit survenir des pannes précoces liées le plus souvent à une malfaçon d'origine, pannes qui sont normalement éliminées par un rodage (wear-in).
- Le milieu de vie, ou vie utile, qui comporte peu de pannes, de taux constant, dont l'apparition reste imprévisible et inéluctable, et pour lesquelles il n'y a donc pas de mesures préventives possibles.
- La fin de vie, qui voit une recrudescence du nombre de pannes dues à l'usure (wear-out), et dont l'apparition peut-être évitée par remplacement préventif des pièces usées (maintenance préventive).

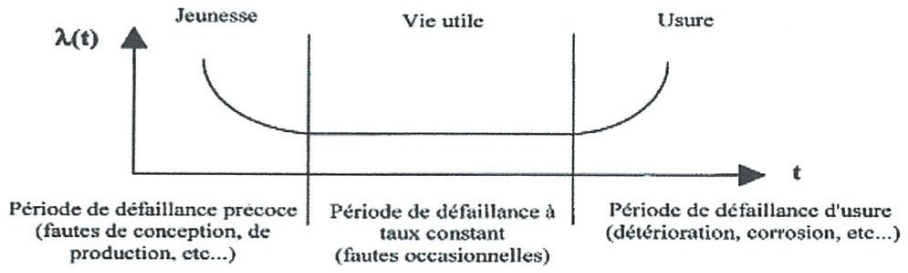


Figure I.4 : Courbe baignoire

Exemple 1.2 *: Les courbes du taux de défaillance des systèmes ont une même forme générale mais présentent néanmoins des différences suivant la technologie principale du système étudié.*

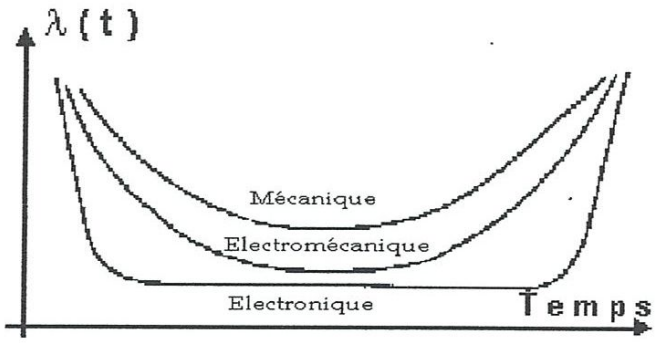


Figure I.5 : Les courbes du taux de défaillance des systèmes

I.5.4 Loi de Fiabilité

Il existe plusieurs manières d'exprimer la fiabilité des systèmes. Les lois les plus utilisés sont :

I.5.4.1 Loi exponentiel

Elle est définie par :

$$R(t) = e^{-\lambda t} \tag{1.5}$$

Cette définition correspond à la fonction densité de probabilité

$$f(t) = \lambda e^{-\lambda t} \tag{1.6}$$

Dans le cas d'un grand nombre d'équipements identiques fonctionnant simultanément, cette probabilité représente donc aussi le taux d'équipements encore en fonctionnement à l'instant t.

Remarque 3

- *Cette remarque est très importante : La fonction exponentielle n'implique ici, en aucune façon, une notion d'usure de matériel ou de diminution d'une grandeur physique (comme par exemple la charge du condensateur dans un circuit RC), et il faut garder présent à l'esprit que la probabilité de panne entre t et (t+ dt) reste constante et égale à λ dt quel que soit t (ce processus n'a pas de "mémoire").*
- *Notons que la défiabilité "unreliability" la fonction $\acute{R}(t) = 1 - R(t)$ qui correspond à la probabilité de tomber en panne avant l'instant t.*
- *MTBF = $1/\lambda i$ avec λi : Taux de défaillance des i constituants ou fonctions élémentaires.*

Ces taux de défaillance seront calculés à partir de retour d'expérience (REX), de résultat d'essais d'endurance, de modèles paramétrés, etc…

La valeur du MTBF est conditionnée par les conditions d'utilisation (Température, stress des composants, fréquence d'utilisation, etc…). Le (ou « la ») MTBF ou MTTF est une grandeur qui permet de calculer une probabilité R(t) de bon fonctionnement au bout d'un temps t.

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

I.5.4.2 Loi de Weibull

Elle est définie par

$$R(t) = \frac{\beta}{\eta}\frac{(t-\gamma)}{\eta}^{\beta-1} \tag{1.7}$$

La fonction densité de probabilité correspondante :

$$f(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}} e^{-\frac{(t-\gamma)^{\beta}}{\eta}} \tag{1.8}$$

Lorsque le taux de défaillance instantané est tel que pour tout réel $t > \gamma$, on a

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t-\gamma}{\eta}\right)^{\beta} \tag{1.9}$$

I.6 Concept de disponibilité

I.6.1 Définitions

i. Aptitude d'un bien, sous les aspects combinés de sa fiabilité, de sa maintenabilité et de l'organisation de la maintenance, à être en état d'accomplir une fonction requise dans des conditions de temps déterminées.

ii. La disponibilité sera la proportion du temps où l'équipement sera opérationnel, l'indisponibilité la proportion où il sera défaillant, ou en étant plus rigoureux, la disponibilité sera la probabilité qu'à un instant le système soit disponible [5].

I.6.1.1 La disponibilité de service

C'est l'aptitude d'un service (service ou mission, fonction à accomplir) à être assuré à l'intérieur de tolérances et dans des conditions spécifiées, à la demande de l'utilisateur.

I.6.1.2 La disponibilité de système

C'est l'aptitude d'un système (sous les aspects combinés de la fiabilité, maintenabilité, logistique de maintenance) à accomplir ou à être en état de remplir une fonction à un instant donné ou dans un intervalle de temps donné.

Pour qu'un équipement présente une bonne disponibilité, il doit :

- Avoir le moins possible d'arrêts de production.
- Etre rapidement remis en bon état s'il tombe en panne.

La disponibilité d'un équipement dépend de nombreux facteurs :

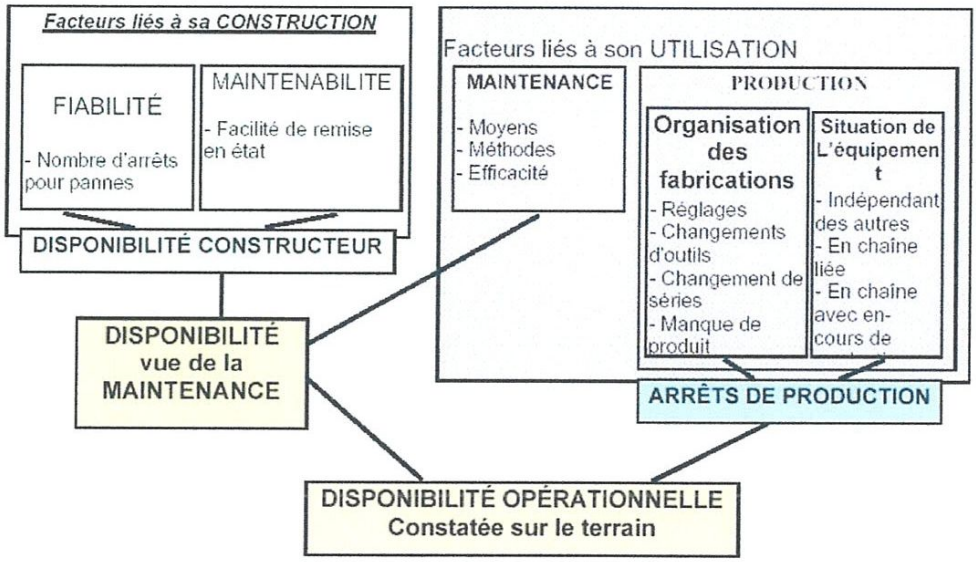


Figure I.6 : Les nombreux facteurs de la disponibilité d'un équipement

Ainsi, la disponibilité d'un système peut s'évaluer selon trois aspects :

- La disponibilité prévisionnelle qui est, de par de sa conception et sa réalisation, l'aptitude théorique d'un bien à accomplir un service.
- La disponibilité théorique qui est en quelque sorte la disponibilité prenant en compte les conditions envahissements et de fonctionnement.

- La disponibilité réelle ou opérationnelle qui est le seul possible à évaluer, à mesurer à partir des données d'activité.

C'est cette dernière qui retient toute l'attention du service maintenance. **La figure I.4** montre tous les composants de la disponibilité réelle dont il est intéressant d'évaluer la participation et sur lesquels il est souhaitable d'agir pour améliorer le résultat global.

Malgré la difficulté apparente, le problème est relativement simple dans le cas d'une machine isolé :

- Pour l'évaluation : Exploitation des historique (MTBF, MTTR, MTTF)
- Pour la correction :
  - ✓ Points de vue conception : Modification, amélioration, re-conception.
  - ✓ Points de vue exploitation : Révision des conditions d'utilisation, gestion de la production, formation de personnel de conduite …
  - ✓ Points de vue maintenance : Révision de la politique de maintenance, amélioration de la logistique, amélioration du niveau d'équipement, formation des techniciens…

La situation est plus complexe dans le cas d'une chaîne de fonctionnement, c'est-à-dire des systèmes installés en ligne avec des dépendances plus ou moins fortes. Dans ces cas, l'indisponibilité d'un poste a souvent des répercussions sur l'ensemble de la ligne.

La détermination de la disponibilité est indispensable pour :

- ➢ Evaluer la possibilité d'assurer le service attendu en fonction des problèmes aléas sur les différents systèmes composants la ligne.
- ➢ Déterminer les besoins d'installation d'un ou plusieurs postes supplémentaires en redondance afin d'améliorer la disponibilité globale.
- ➢ Rechercher les postes (simples ou doubles) présentant globalement une disponibilité pénalisante afin d'agir ponctuellement.
- ➢ Mettre en évidence la nécessité d'en-cours (stocks intermédiaires) pour minimiser le risque de blocage complet en cas de défaillance isolée [5].

La disponibilité allie donc les notions de fiabilité et de maintenabilité. Augmenter la disponibilité passe par :

- L'allongement de la MTBF (action sur la fiabilité).
- La notion de le MTTR (action sur la maintenance).

I.6.2 Fonction de disponibilité

I.6.2.1 La disponibilité instantanée

D(t) est l'aptitude (probabilité) d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée. Elle prend en compte à la fois la fiabilité et la maintenabilité.

Pour la modélisation nous nous plaçons dans l'hypothèse exponentielle, avec les deux taux λ et μ supposés constant et indépendants du temps.

La disponibilité instantanée d'un systéme réparable est de la forme:

$$D(t) = \mu/\mu + \lambda + \lambda/\mu + \lambda \cdot e^{-(\mu+\lambda)t} \qquad (1.10)$$

Avec μ est le taux de réparation: μ=1/MTTR et λ=1/MTBF

La disponibilité est le plus souvent estimée à partir de sa valeur asymptotique définie par la formule :

- **Disponibilité intrinsèque Di**

$$D_i = \frac{MTBF}{MTBF + MTTR} = \frac{\mu}{\lambda + \mu} \qquad (1.11)$$

- **Disponibilité opérationnelle Do**

$$D_0 = \frac{MTBF}{MTBF + MTTR + MTL} \qquad (1.12)$$

MTL: moyenne des temps logistiques.

- **Disponibilité en mission**

$$D = [1/(t_2 - t_1)] \int_{t1}^{t2} D(t)\,dt \qquad (1.13)$$

- **Disponibilité moyenne est la valeur limite de la précédente**

$$D = \lim_{T \to \infty} \left[\left\{ \int_0^T D(t)\, dt \right\} / T \right] \quad (1.14)$$

Le MTBF n'est défini que pour des systèmes réparables donc pas des composants.

Le taux de disponibilité, au cours du temps, est défini par:

$$D = D(t) = \frac{\text{Temps d'utilisation et d'attente}}{\text{Temps d'utilisation et d'attente + Temps de maintenance}} \quad (1.15)$$

Indisponibilité = 1 - disponibilité = 1 - D.

I.6.3 Paramètres ayant une influence sur la disponibilité

- Dispositif (description) : Nombre d'équipements, sous-ensembles interchangeables, décomposition en sous-ensembles interchangeables, redondances actives ou passives, reconfigurations possibles, renouvellement ...
- Conditions d'utilisation : Environnement, contraintes (thermiques, ...), mise sous tension; nombre de dispositifs, taux d'activité de chaque partie, motivation des divers utilisateurs, motivation du personnel de maintenance, possibilité de réparer en temps masqué ...
- MTBF et Taux de défaillance : Loi de mortalité, maladies de jeunesse, pannes communes ...
- Choix de la politique de maintenance : Maintenance corrective ou préventive, échelon des opérations de maintenance ...
- Temps de maintenance : Opérations, vérifications, diagnostic, remplacement, réparations, logistique ...
- Aptitude à la réparation : Accessibilité, démontabilité, remontabilité ...
- Testabilité : Tester ou surveiller, localiser les pannes ...
- Gestion des rechanges : Stocks, quantités stockées, réapprovisionnement, rupture de stock, répartition géographique ...
- Aspects humains : Conditions de travail (stress, fatigue ...), formation, motivation ...
- Interactions extérieures : Météo, poussière, atmosphère saline, incendie, erreurs humaines, accidents ...

- Coûts : Acquisition, stock de rechange, matériel de maintenance, salaires, frais généraux, coûts de maintien ...

I.7 Fiabilité et disponibilité des systèmes complexes

I.7.1 Redondance

On distingue essentiellement :

- La redondance active ou chaude : Dans laquelle tous les moyens sont mis en œuvre simultanément. Elle peut être totale (il suffit qu'un seul moyen fonctionne) ou majoritaire (m moyens doivent fonctionner parmi les n).
- La redondance passive ou froide : (Séquentielle, en attente, de réserve) dans laquelle une défaillance, de façon non instantanée, en principe par intervention humaine. Elle peut se faire simplement par remplacement d'un sous-ensemble sans avoir à se préoccuper de la réparation éventuelle du sous-ensemble défaillant.

Selon les cas, les données de fiabilité à utiliser concerneront les dispositifs en fonctionnement en stockage, en mode dormant ou en mode marche/arrêt.

1.7.2 Systèmes en série

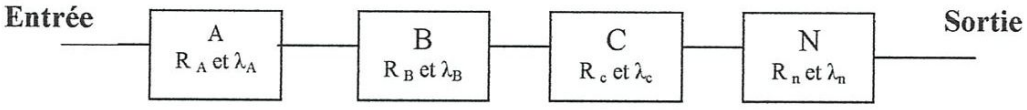


Figure I.7 : Système en série

Un système en série fonctionne si et seulement si chaque composant fonctionne. Donc pour un système en série constitué de *k* composants on a

$$S = A \cap B \cap .... \cap N \qquad (1.16)$$

Si les composants du système fonctionnent indépendamment les uns des autres la probabilité que le système fonctionne est donnée par

$$P(S) = P(A) \times P(B) \times ..... P(N) \qquad (1.17)$$

La fiabilité Rs d'un ensemble de n constituants connectés en série est égale au produit des fiabilités respectivement R_A, R_B, R_C,.....R_n. de chaque composant.

On a donc :

$$R_S = R_A \times R_B \times \ldots\ldots\ldots\ldots R_n \quad (1.18)$$

Si les n composantes sont identiques et tous de même fiabilité R, alors

$$R_S = (R)^n \quad (1.19)$$

Si les taux de défaillances sont constants au cours du temps, la fiabilité sera calculée suivant la formule :

$$R(s) = (e^{-\lambda A t}) \times (e^{-\lambda B t}) \times (e^{-\lambda C t}) \times \ldots\ldots \times (e^{-\lambda n t}) \quad (1.20)$$

Avec :

$$MTBF_S = \frac{1}{\lambda_a + \lambda_b + \lambda_c + \ldots\ldots\ldots\ldots + \lambda_n} \quad (1.21)$$

Si en plus, les composantes sont identiques : $\lambda_A, \lambda_B, \ldots, \lambda_n = \lambda$

$Rs = e^{-n\lambda t}$ et $MTBFs = 1/n\lambda$.

Cas de la disponibilité globale de n unité indépendante en série : la disponibilité résultante du système est le produit :

$$D_s = D_A \times D_B \times \ldots\ldots\ldots\ldots D_n = \Pi D_i \quad (1.22)$$

Exemple 1.3 : *Soient deux unités de disponibilité 0,90 et 0,80 en série, alors :*

Ds=0,9 ×0,8=0,72.

I.7.3 Systèmes en parallèle

La fiabilité d'un système peut être augmentée en plaçant en parallèle. Un dispositif constitué de n composants en parallèle ne peut tomber en panne que si les n tombent en panne au même moment.

Si F_i est la probabilité de panne d'un composant, la fiabilité associée R_i est son complémentaire: $Fi = 1-R_i$.

Soit les "n" composants de la figure ci –dessous montés en parallèle de panne pour chaque composant repéré (i) est notée Fi, alors :

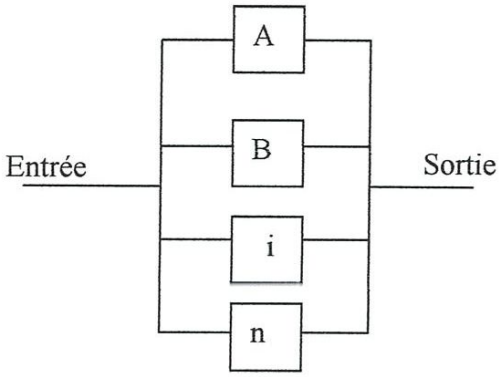


Figure I.8 : Système en parallèle

Un système en parallèle fonctionne si et seulement si au moins un composant fonctionne. Donc pour un système en parallèle constitué de k composants on a

$$S = A \cup B \cup \ldots\ldots\ldots \cup n \tag{1.23}$$

la probabilité de pannes f(p) de l'ensemble des « n » composants en parallèle est égal au produit des F_i entre eux :

$$F_p = F_1 \times F_2 \times F_n = (1 - R_1) \times (1 - R_2) \times \ldots\ldots\ldots\ldots\ldots\ldots \times (1 - R_n) \tag{1.24}$$

Si les composants du système fonctionnent indépendamment les uns des autres la probabilité que le système fonctionne est donnée par :

$$P_p = 1 - (1 - P(A_1)) \times (1 - P(A_2)) \times \ldots\ldots\ldots\ldots\ldots (1 - P(A_k)) \tag{1.25}$$

La fiabilité Rp de l'ensemble est donnée par la relation :

$$R_p = 1 - (1 - R_1) \times (1 - R_2) \times (1 - R_3) \times (1 - R_4) \times \ldots\ldots\ldots\ldots (1 - R_N) \tag{1.26}$$

Si les « n » composants sont identiques ($R=R_1=R_2=\ldots\ldots=R_n$) et ont tous ma même fiabilité R. L'expression devient :

$$R(p) = 1 - (1 - R)^n \tag{1.27}$$

La disponibilité de n unités indépendantes en parallèle se calcule de la même manière que la fiabilité.

Notons l'indisponibilité I=1-D, nous obtenons :

$$I = 1 - D_p = (1 - D_A) \times (1 - D_B) \times \ldots\ldots\ldots (1 - D_n) \qquad (1.28)$$

Exemple 1.4 : *Soient deux unités de disponibilités 0,90 et 0,80 en parallèle, alors :*

$1-D_p= (1-0,9) (1-0,8)=0,02.$
$D_p=0,98.$

I.7.4 Série parallèle

C'est la combinaison des deux cas précédents

Exemple 1.5 : *soit l'association de composants ci dessous, avec leur fiabilité respective.*

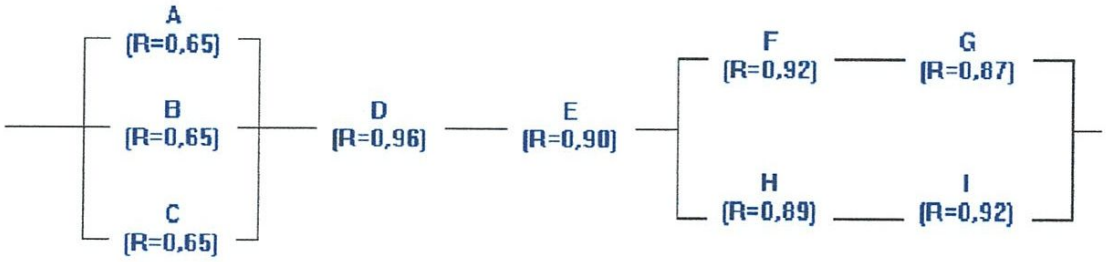


Figure I .9 : Système Série parallèle

La fiabilité globale est :

$$R(t) = [1 - (1 - R_A)(1 - R_B)(1 - R_C)] \times R_D \times R_E \times [1 - (1 - R_F \times R_G)(1 - R_H \times R_I)]$$

R(t)=O,47=47% .

I.8 Maintenabilite

La maintenabilité M(t) est, dans des conditions données d'utilisation, l'aptitude (la probabilité) d'une entité à être maintenue ou remise en service sur un intervalle donné de temps, 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.

Le taux instantané de remise en service μ(t) d'un dispositif est la densité de probabilité pour qu'il soit remis en service entre les instants t et t+dt sachant qu'il était en panne à l'instant t.

$\mu(t) = dM(t) / [1- M(t)]\, dt$

$$M(t) = 1 - e^{-\int_0^t \mu(\tau) d\tau} \tag{1.29}$$

Le temps moyen avant remise en service MTTR (*Mean Time To Repair*) est donné par :

$$MTTR = \int_a^\infty [1 - M(t)]dt \tag{1.30}$$

I.9 Sécurité

La sécurité c'est l'aptitude d'un produit à respecter, pendant toutes les phases de vie, un niveau acceptable de risques d'accident susceptible d'occasionner une agression du personnel ou une dégradation majeure du produit ou de son environnement. Elle représente l'absence de conséquence catastrophique pour l'environnement [2].

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

La notion de sécurité est étroitement liée à celle du risque qui lui –même dépend non seulement de la probabilité d'occurrence mais aussi de la gravité de l'événement.

On peut accepter de risquer sa vie, grande gravité, si la probabilité d'occurrence est assez faible .si le risque est uniquement de se casser une jambe on peut accepter une probabilité plus grande.

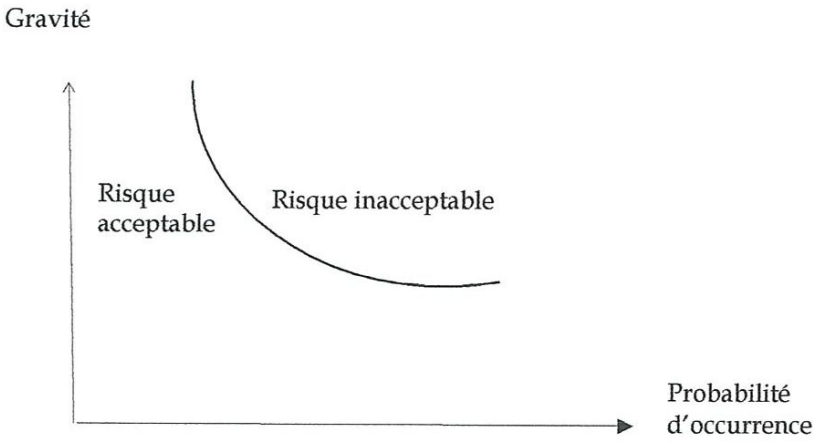


Figure I.10 : Le niveau de risque est fonction du couple, gravité, probabilité d'occurrence

I.10 Conclusion

Nous avons introduit, en premier lieu, les concepts de sûreté de fonctionnement, et notamment les paramètres Fiabilité, Maintenabilité, Disponibilité et Sécurité. Ces paramètres sont interdépendants et la prise en compte simultanément de ceux-ci doit être incluse dès la conception du système. Leur connaissance présente un intérêt majeur dans le monde industriel et il est nécessaire de pouvoir les évaluer tout au long du cycle de vie du système pour des raisons économiques et pour limiter les risques potentiels sur le système et son environnement, suite à d'éventuels dysfonctionnements [1].

Chapitre 2

Méthode d'analyse de la Sureté de Fonctionnement

II.1 Introduction

Dans ce chapitre, nous présentons les différentes méthodes d'analyse de la sureté de fonctionnement des systèmes, avant de définir ces méthodes on définir la notion de scénario redouté.

II.2 Scénario redouté

Définissons tout d'abord ce que c'est qu'un scénario. Un scénario sous-entend un début, une fin et une histoire qui décrit l'évolution d'un système. Dans le contexte de la sûreté de fonctionnement, un scénario redouté mène à un état catastrophique ou dangereux: c'est l'état final (dit état redouté). L'état initial est un état de bon fonctionnement du système. Le scénario redouté décrit de manière précise (ce qui est nécessaire pour la compréhension) et

concise (le juste nécessaire: causalité) comment le système quitte le bon fonctionnement pour évoluer vers un fonctionnement jugé dangereux. C'est en effet une description du système sous la forme de changements d'états et de suites d'événements qui mènent vers l'état redouté. C'est une explication claire des raisons pour lesquelles le système s'est trouvé ou risque de se trouver dans un état redouté donné.

En résumé, un scénario redouté est une description de l'évolution de certains composants du système global à partir d'un état de bon fonctionnement jusqu'à l'occurrence de l'événement redouté. Ce scénario fait donc intervenir uniquement les composants ayant un lien de causalité avec l'occurrence de l'événement redouté [6].

II.3 L'analyse fonctionnelle

Pour analyser les défaillances d'un système, il est nécessaire auparavant de bien identifier à quoi doit servir ce système : c'est à dire de bien identifier toutes les fonctions que ce système doit remplir durant sa vie de fonctionnement et de stockage.

D'après la norme (AFNOR NF X 50-151), l'analyse fonctionnelle est une démarche qui consiste à rechercher, ordonner, caractériser, hiérarchiser et / ou valoriser les fonctions du produit (matériel, logiciel, processus, service) attendues par l'utilisateur.
Une fonction est l'action d'un élément constitutif d'un système exprimée exclusivement en terme de finalité (par ce qu'il « fait »). Chaque fonction doit être exprimée, formulée, par un verbe à l'infinitif suivi d'un ou plusieurs compléments.
L'analyse fonctionnelle est utilisée au début d'un projet pour créer (conception) ou améliorer (reconception) un produit. Elle est un élément indispensable à sa bonne réalisation. On détermine donc, par exemple, les fonctions principales, les fonctions secondaires et les fonctions contraintes d'un produit. Il est important de faire ce recensement afin d'effectuer un dimensionnement correct des caractéristiques du produit.
Une analyse fonctionnelle, précède donc une étude de sûreté de fonctionnement. Une première analyse fonctionnelle dite externe permet de définir avec précision les limites matérielles du système étudié, les différentes fonctions et opérations réalisées par le système ainsi que les diverses configurations d'exploitation. L'analyse fonctionnelle interne permet de réaliser une décomposition arborescente et hiérarchique du système en éléments matériels et/ou fonctionnels. Elle décrit également des fonctions dans le système [7].

II.4 L'Analyse préliminaire des risques

L'Analyse Préliminaire des Risques (APR) est une extension de l'Analyse Préliminaire des Dangers (APD). Elle est réalisée après l'analyse fonctionnelle. Elle a pour but d'établir une liste aussi exhaustive que possible des incidents ou accidents pouvant avoir des conséquences sur la sécurité du personnel ou du matériel. Un autre objectif de L'*APR* est d'évaluer la gravité des conséquences liées aux situations dangereuses et les accidents potentiels.

La méthode permet de recenser les dangers et déduire ensuite tous les moyens et toutes les actions correctrices permettant d'éliminer ou de maîtriser les situations dangereuses et les accidents potentiels. Il est recommandé de commencer l'APR dès les premières phases de la conception. Cette analyse sera vérifiée et complétée au fur et à mesure de l'avancement dans la réalisation de système. L'APR permet de mettre en évidence les événements redoutés critiques qui devront être analysés en détail dans la suite de l'étude de sûreté de fonctionnement, en particulier par la méthode des arbres de défaillances [8].

II.5 Présentation de la méthode AMDEC

L'analyse des Modes de Défaillance, de leurs Effets et de leurs criticité (AMDEC, en anglais, FMECA/FMEA : Failure Mode Effects and Criticality Analysis) est développée initialement par l'armée américaine. La référence Militaire MIL-P-1629, intitulé "Procédures pour l'Analyse des Modes de Défaillance, de leurs Effets et de leurs Criticités", est datée du 9 Novembre 1949. C'est une extension de l'analyse des Modes de Défaillance et de leurs Effets (AMDE).

Cette La méthode était employée comme une technique d'évaluation des défaillances afin de déterminer la fiabilité d'un équipement et d'un système. Les défaillances étaient classées selon leurs impacts sur le personnel et la réussite des missions pour la sécurité de l'équipement. Le concept personnel et équipement interchangeables ne s'applique pas dans le monde moderne de fabrication des biens de consommation. Les fabricants de produits de consommation ont établi de nouvelles valeurs telles que la sécurité et la satisfaction client.

L'AMDEC a été employée pour la première fois à partir des années 1960 dans le domaine de l'aéronautique pour l'analyse de la sécurité des avions. La mise en œuvre s'est longtemps limitée à l'utilisation dans le cadre d'études de fiabilité du matériel. Son utilisation s'est depuis largement répandue à d'autres secteurs d'activités telles que l'industrie chimique, pétrolière ou le nucléaire. De fait, elle est essentiellement adaptée à l'étude des défaillances de

matériaux et d'équipements et peut s'appliquer aussi bien à des systèmes de technologies différentes (systèmes électriques, mécaniques, hydrauliques...) qu'à des systèmes alliant plusieurs techniques.

A la fin des années soixante-dix, la méthode fut largement adoptée par Toyota, Nissan, Ford, BMW, Peugeot, Volvo, Chrysler et d'autres grands constructeurs d'automobiles.
En 1988, L'ISO émettait les normes de la série ISO 9000. Le QS 9000 est l'équivalent de l'ISO 9000 pour l'automobile. Un groupe de travail représentant entre autre Chrysler a développé le QS 9000 pour standardiser les systèmes qualité des fournisseurs. Conformément au QS 9000, les fournisseurs automobiles doivent utiliser la planification qualité du procédé (APQP), incluant l'outil AMDEC et développant les plans de contrôle.

L'AIAG (Automotive Industry Action Group) et l'ASQC (American Society for Quality Control) émettent les normes AMDEC en février 1993. Les normes sont présentées dans un manuel de l'AMDEC approuvé et soutenu par trois constructeurs automobiles. Ce manuel fournit les principes généraux pour préparer une AMDEC.

Bien qu'ayant subi de nombreuses critiques dues au coût et à la lourdeur de son application, elle reste néanmoins une des méthodes les plus répandues et l'une des plus efficaces. Elle est en effet de plus en plus utilisée en sécurité, maintenance et disponibilité non seulement sur le matériel, mais aussi sur le système, le fonctionnel et le logiciel.
Aussi est-elle maintenant largement recommandée au niveau international et systématiquement utilisée dans toutes les industries à risque, comme le nucléaire, le spatial, la chimie, agroalimentaire et autres dans le but de faire des analyses préventives de la sûreté de fonctionnement.

II.5.1 Principes généraux de la méthode AMDEC

L'AFNOR (Association Française de NORmalisation) définit l'AMDEC comme étant : Une méthode inductive qui permet de réaliser une analyse qualitative et quantitative de la fiabilité ou de la sécurité d'un système.

La méthode AMDEC est avant tout une méthode d'analyse de systèmes (systèmes au sens large composé d'éléments fonctionnels ou physiques, matériels, logiciels, humains ...), statique, s'appuyant sur un raisonnement inductif (causes - conséquences), pour l'étude organisée des causes, des effets des défaillances et de leur criticité.

La méthode AMDEC consiste à examiner méthodiquement les défaillances potentielles des systèmes - analyse des modes de défaillances-, leurs causes et leurs conséquences sur le fonctionnement de l'ensemble, leurs effets.

L'analyse des Modes de Défaillance et de leurs Effets repose notamment sur les concepts de [3]:

- Défaillance, soit la cessation de l'aptitude d'un élément ou d'un système à accomplir une fonction requise.
- Mode de défaillance, soit l'effet par lequel une défaillance est observée sur un élément du système.
- Cause de défaillance, soit les évènements qui conduisent aux modes de défaillances.
- Effet d'un mode de défaillance, soit les conséquences associées à la perte de l'aptitude d'un élément à remplir une fonction requise.

En pratique, il est souvent difficile de bien distinguer ces différentes notions. La maîtrise de ce vocabulaire est néanmoins primordiale pour une bonne utilisation de cet outil. Pour illustrer ces différents concepts, prenons l'exemple d'une pompe. Dans des conditions normales d'exploitation, la fonction de cette pompe est sera définie comme son aptitude à fournir un débit donné à sa sortie. Si le débit en sortie de pompe est nul, nettement inférieur ou supérieur à ce débit défini, la pompe sera dite « défaillante ». Si, en cours d'exploitation, la pompe s'arrête de façon non désirée, on assistera bien à une défaillance de la pompe. Le fait que la pompe s'arrête constitue donc un effet par lequel une défaillance est observée, il s'agit d'un mode de défaillance. La coupure de courant qui a entraîné l'arrêt de la pompe sera alors définie comme une des causes de ce mode de défaillance. L'arrêt de l'approvisionnement du réacteur alimenté par cette pompe suivie d'une dégradation du produit de synthèse constituera des conséquences de cette défaillance. L'AMDE est une méthode inductive d'analyse qui permet :

- D'évaluer les effets et la séquence d'évènements provoqués par chaque mode de défaillance des composants d'un système sur les diverses fonctions de ce système.
- Déterminer l'importance de chaque mode de défaillance sur le fonctionnement normal du système et en évaluer l'impact sur la fiabilité, la sécurité du système considéré.
- Hiérarchiser les modes de défaillances connus suivant la facilité que l'on a à les détecter et les traiter.

Lorsqu'il est nécessaire d'évaluer la criticité d'une défaillance (probabilité et gravité), l'Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité (AMDEC) apparaît comme une suite logique à l'AMDE. L'AMDEC reprend en effet les principales étapes de l'AMDE et y ajoute une évaluation semi quantitative de la criticité. Cette dernière peut par exemple être réalisée sur la base des échelles appropriées.

II.5.2 Définition des termes relatifs à la méthode AMDEC

L'AMDEC est une technique d'analyse prévisionnelle, s'applique notamment au produit ou au processus, permettant d'estimer les risques d'apparition des défaillances et de leurs conséquences.

Chaque défaillance est caractérisée par :

- La gravité (G ou S) perçue par " le client/consommateur ".
- La fréquence d'apparition (F ou O).
- Le risque de non-détection d'une défaillance (D).

On définit alors un « Niveau de Priorité de Risque » (NPR = FxGxD). Après une hiérarchisation des défaillances potentielles, basée sur le NPR, des actions prioritaires sont déclenchées, réalisées et suivies.

Criticité : La criticité est le produit mathématique de l'évaluation de l'Occurrence et de la Sévérité. Criticité = (S) × (O). Ce nombre est employé en priorité pour des éléments nécessitant un niveau de qualité supérieur.
Contrôles : Les contrôles (conception et procédé) sont les mécanismes empêchant la cause d'une défaillance de survenir.
Clients : Les clients sont externes et internes, le personnel et les procédés qui seront concernés par la défaillance du produit. Le Client pourrait être la prochaine opération, opérations ultérieures, ou l'utilisateur final.
Détection : La détection est une évaluation de la probabilité que les contrôles (conception et procédé) détecteront la cause d'une défaillance ou la défaillance elle-même.
Défaillance : Une défaillance se présente lorsqu'un produit, un composant ou un ensemble : Ne fonctionne pas, ne fonctionne pas au moment prévu, ne s'arrête pas au moment prévu, fonctionne à un instant non désiré ou fonctionne, mais les performances requises ne sont pas obtenues.

Modes de défaillance : La façon dont un produit, un composant, un processus manifeste une défaillance ou s'écarte des spécifications. Ce mode peut prendre l'une des formes suivantes : Une déformation, vibration, coincement, desserrage, corrosion, fuite, perte de performance, court-circuit, flambage, difficulté à s'arrêter ou à démarrer, dépassement de la limite supérieure tolérée, etc. Les modes de défaillance sont parfois décrits comme des catégories de défauts. Un mode de défaillance potentiel décrit la façon dans laquelle un produit ou un procédé pourrait échouer dans l'exécution de sa fonction première.

Causes de défaillance : Les causes de défaillance (amont) sont les circonstances associées à la conception, à la fabrication ou à l'utilisation, qui ont entraînés une défaillance.

Effets de défaillance : Les effets d'une défaillance (aval) sont les symptômes par lequel est décelée l'altération ou la cessation d'une fonction requise, et qui en est la conséquence.

Éléments AMDEC : Les éléments AMDEC sont identifiés ou analysés dans le cadre du procédé AMDEC. Les exemples communs sont: Les fonctions, les modes de défaillance, les causes, les effets, les contrôles, et Actions. Les éléments AMDEC deviennent les titres de colonne du formulaire.

Fonction : Une fonction pourrait être le but d'un produit ou d'un procédé. Les fonctions AMDEC sont décrites dans la forme verbale.

Occurrence (Fréquence d'apparition) : L'occurrence est une évaluation de l'apparition d'une défaillance particulière (à l'utilisation, la fabrication ou à la conception d'un produit).

Nombre Prioritaire de Risque (NPR) : Le nombre prioritaire de risque est le produit de la Sévérité, de l'Occurrence, de la Détection. NPR = (S) * (O) * (D). Ce nombre est employé prioritairement sur des articles qui nécessité un niveau de qualité supérieur.

Sévérité (Gravité) : La sévérité (ou la gravité) est une évaluation de l'importance de l'effet de la défaillance potentielle sur le Client.

Caractéristiques spéciales du processus : Les caractéristiques spéciales du procédé sont des caractéristiques pour lesquelles les variations doivent être contrôlées par rapport à une valeur cible pour assurer une caractéristique spéciale du produit. Cette variation est entretenue à sa valeur cible pendant la fabrication et l'assemblage.

Caractéristiques spéciales du produit : Les caractéristiques spéciales du produit sont des caractéristiques pour lesquelles une variation prévue pourrait considérablement concerner la sécurité d'un produit ou la conformité à des règlements ou des normes gouvernementales.

II.5.3 Les types AMDEC et leur utilisation

AMDE / AMDEC s'applique à un produit ou à un procédé

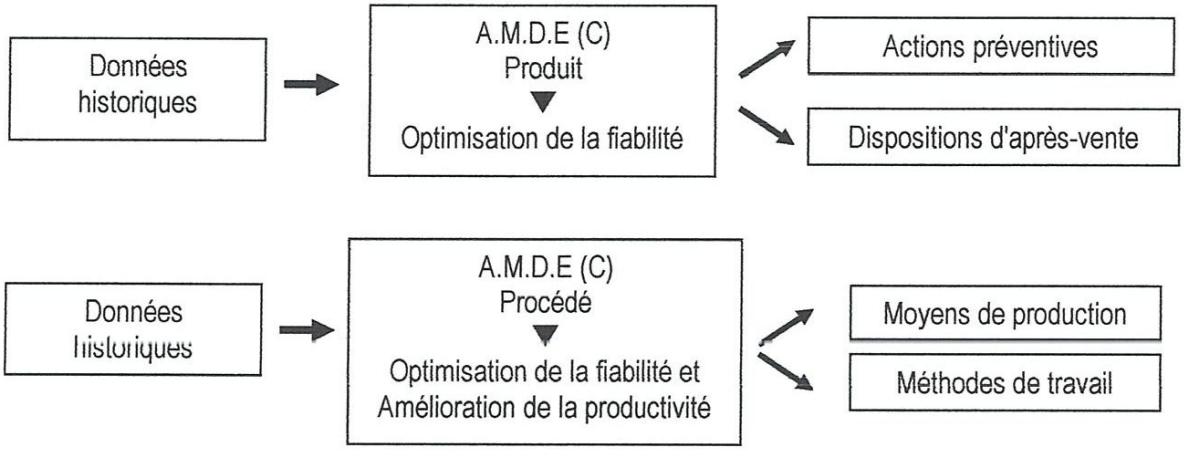


Figure II.1 : Les types AMDEC

Il existe plusieurs types AMDEC selon l'usage prévu :

- AMDEC organisation s'applique aux différents niveaux de processus principaux de l'entreprise : Du premier niveau qui englobe les processus de gestion, d'information, de production, de gestion du personnel et le processus marketing, jusqu'au dernier niveau comme l'organisation d'une tâche de travail.
- AMDEC produit ou projet est utilisée pour étudier en détail la phase de conception du produit ou d'un projet. Si le produit comprend plusieurs composants, on applique des AMDEC sur les composants.
- AMDEC processus s'applique à des processus de fabrication. Elle permet d'analyser et évaluer la criticité de toutes les défaillances potentielles d'un produit engendrées par son processus. Elle peut être utilisée pour les postes de travail.
- AMDEC moyen s'applique à des machines, outils, équipements et appareils de mesure, des logiciels et systèmes de transport interne.
- AMDEC service s'applique pour vérifier que la valeur ajoutée réalisée dans le service correspond aux attentes des clients et que le processus de réalisation de service n'engendre pas de défaillances.
- AMDEC sécurité s'applique pour assurer la sécurité des opérateurs dans les procédés où existent des risques pour ceux-ci.

II.5.4 Méthodologie

Avant de se lancer dans la réalisation proprement dite des AMDEC, il faut connaître précisément le système et son environnement. Ces informations sont généralement les résultats de l'analyse fonctionnelle, de l'analyse des risques et éventuellement du retour d'expériences.

Il faut également déterminer comment et à quel fin l'AMDEC sera exploitée et définir les moyens nécessaires, l'organisation et les responsabilités associées.

Dans un second temps, il faut évaluer les effets des modes de défaillance. Les effets de mode de défaillance d'une entité donnée sont étudiées d'abord sur les composants directement interfacés avec celui-ci (effet local) et de proche en proche (effets de zone) vers le système et son environnement (effet global).

Il est important de noter que lorsqu'une entité donnée est considérée selon un mode de défaillance donné, toutes les autres entités sont supposées en état de fonctionnement nominal.

Dans un troisième temps, il convient de classer les effets des modes de défaillance par niveau de criticité, par rapport à certains critères de sûreté de fonctionnement préalablement définis au niveau du système en fonction des objectifs fixés (fiabilité, sécurité, etc.).

Les modes de défaillance d'un composant sont regroupés par niveau de criticité de leurs effets et sont par conséquent hiérarchisés.

Cette typologie permet d'identifier les composants les plus critiques et de proposer alors les actions et les procédures " juste nécessaires " pour y remédier. Cette activité d'interprétation des résultats et de mise en place de recommandations constitue la dernière étape de l'AMDEC.

II.5.5 Étapes de mise en place de l'AMDEC

Avant d'entamer la mise en place proprement dite de l'AMDEC, il faut satisfaire certaines conditions préliminaires considérées comme essentielles pour la réussite d'une analyse AMDEC.

II.5.5.1 Conditions préliminaires

L'utilisation **de l'**AMDEC nécessite au préalable :

- La formation de tous les acteurs potentiels et de l'animateur de l'équipe.
- Formation de l'équipe à l'utilisation des outils de travail de groupe (Pareto, Ishikawa, etc.).
- Désignation d'un pilote pour les actions AMDEC, directement rattaché à la direction.
- Prévoir les moyens nécessaires : L'analyse AMDEC nécessite beaucoup de temps (8 à 40 heures, voir plus) pour chaque intervenant ou participant, et le double pour l'animateur.
- Disponibilité des membres de l'équipe.
- Rigueur pour le respect de la procédure de référence et suivi des actions correctives.

II.5.5.2 Les principales étapes de la mise en place de l'AMDEC

Les principales étapes de la mise en place d'une démarche AMDEC sont les suivantes :

- Poser le problème : Définir clairement l'objectif à atteindre et le champ d'application.
- Définir le demandeur et le décideur : Le demandeur peut être, par exemple, le client qui cherche à s'assurer que tous les risques sont identifiés. Le décideur, c'est le chef du projet qui accepte ou non les exigences du client et identifie le sujet, le délai et le budget alloué à l'étude.
- Constituer l'équipe AMDEC : L'équipe doit être pluridisciplinaire et elle est composée de l'animateur, qui est le garant de la méthode AMDEC, et de représentants de différentes fonctions concernées. Il est préférable que l'animateur ne soit pas le concepteur du processus (ou autre) objet de l'étude.
- Analyse fonctionnelle : Le système est décomposé en sous systèmes, et ceux-ci en composants élémentaires. Pour chaque élément on détermine les fonctions principales (à quoi ça sert) et les fonctions contraintes (lois, règlements, normes, etc.).
- Analyse qualitative des défaillances : Recensement des modes de défaillance, des causes qui sont à l'origine (Causes de défaillance) et de leur effet (Effet de défaillances).
- Analyse quantitative des défaillances : Pour chaque mode de défaillance, évaluer la gravité, la fréquence d'apparition, le risque de non-détection et calculer le nombre prioritaire de risque (NPR).

- Déterminer le NPR critique : Après l'hiérarchisation des modes de défaillance selon leur NPR, on détermine le NPR au-dessus duquel il faut déclencher des mesures correctives.
- Plan d'action : Préparer un plan d'action (quoi, qui, comment, quand) pour supprimer les causes de défaillances. Les actions peuvent être d'ordre préventif ou correctif.
- Application et suivi du plan d'action : Les responsables désignés sur le plan d'action sont chargés d'appliquer et suivre les mesures correctives (ou préventives) et d'enregistrer les résultats obtenues.
- Vérification de l'efficacité des solutions : La mise en œuvre des solutions est suivie d'une vérification de leur efficacité. Au cas où les solutions ne permettent pas d'atteindre les effets escomptés, il faut reprendre une nouvelle analyse et définir de nouvelles solutions. (Voir annexe A).

Dans les faits, il est intéressant de se doter de tableaux tant en qualité de support pour mener la réflexion que pour la présentation des résultats [3].

- Equipement (colonne 1)

Concrètement, il s'agit de passer en revue chaque équipement ou composant identifié lors de la description fonctionnelle. Il est généralement utile de repérer l'équipement considéré à partir des données fournies dans des diagrammes ou autres plans.

- Fonction et états (colonne 2)

Pour chacun des équipements, il s'agit de lister ses fonctions et états de fonctionnements. Ces fonctions et états sont normalement identifiés au cours de la description fonctionnelle. Afin de mener l'analyse de la manière la plus complète possible, il est indispensable de considérer l'ensemble des états susceptibles de survenir au cours de l'exploitation (ex. fonctionnement normal, arrêt, démarrage, stand-by...).

- Modes de défaillance (colonne 3)

Pour chaque équipement et en fonction de l'état de fonctionnement, le groupe de travail doit envisager de manière systématique les modes de défaillances possibles (Colonne 3). La définition des modes possibles de défaillance pour un équipement peut être réalisée à partir du retour d'expérience associé à l'exploitation d'équipements similaires, de tests ou essais... Par ailleurs, les modes de défaillance considérés devront tenir compte :

- Des utilisations du système.

- Des caractéristiques de l'équipement considéré.
- Du mode de fonctionnement.
- Des spécifications relatives au fonctionnement.
- Des délais fixés.
- De l'environnement.

Quel que soit le type d'équipement considéré, la liste suivante tirée de la norme CEI 60812:1985: « Techniques d'analyse de la fiabilité des systèmes - Procédure d'analyse des modes de défaillance et de leurs effets (AMDE) » facilite l'identification des modes de défaillance par le groupe de travail.

1	Fonctionnement prématuré
2	Ne fonctionne pas au moment prévu
3	Ne s'arrête pas au moment prévu
4	Défaillance en fonctionnement

Tableau II.1 : Modes de défaillance généraux

De plus, cette même norme propose une liste guide de modes de défaillance génériques, qui permet d'aider le groupe de travail dans l'analyse. Cette liste est reprise ci-après. Elle présente une série de modes de défaillance générique pouvant s'appliquer en théorie à tous les cas de figure envisageables. Néanmoins, elle pourra être utilement complétée en vue de tenir compte des spécificités du système étudié.

1	Défaillance structurelle (rapture)	18	Mise en marche erronée
2	Blocage physique ou coincement	19	Ne s'arrête pas
3	Vibrations	20	Ne démarre pas
4	Ne reste pas en position	21	Ne commute pas
5	Ne s'ouvre pas	22	Fonctionnement prématuré
6	Ne se referme pas	23	Fonctionnement après le délai prévu (retard)
7	Défaillance en position ouverte	24	Entrée erronée (augmentation)
8	Défaillance en position fermée	25	Entrée erronée diminution)
9	Fuite interne	26	Sortie erronée (augmentation)
10	Fuite externe	27	Sortie erronée (diminution)
11	Dépasse la limite supérieure tolérée	28	Perte de l'entrée
12	Est en dessous de limite inférieure tolérée	29	Perte de la sortie
13	Fonctionnement intempestif	30	Court-circuit (électrique)
14	Fonctionnement intermittent	31	Circuit ouvert (électrique)
15	Fonctionnement irrégulier	32	Fuite (électrique)
16	Indication erronée	33	Autres conditions de défaillance exceptionnelles suivant les caractéristiques du système, les conditions de fonctionnement et les contraintes opérationnelles

Tableau II.2 : Modes de défaillance génériques

- Cause de défaillance (colonne 4)

Pour chaque mode de défaillance, le groupe de travail doit ensuite identifier les causes potentielles conduisant à ce mode de défaillance. Un mode de défaillance peut résulter de plusieurs causes, qu'il convient donc d'inventorier et de numéroter pour plus de facilité. La liste présentée dans le **Tableau II.8** précédent permet également de préciser des causes de défaillance dans la mesure où ces causes peuvent parfois s'apparenter à des modes de défaillance. Par exemple, un mode de défaillance d'une vanne devant se fermer peut être « Ne se ferme pas » (mode de défaillance n°6). Une des causes de ce mode de défaillance peut être un blocage physique ou coincement (mode de défaillance n°2). Enfin, il convient de tenir compte des défaillances possibles sur les équipements adjacents du système. L'évaluation des

effets d'une défaillance d'un élément peut effectivement conduire à l'occurrence d'un mode de défaillance sur un autre élément du système. Il est ainsi nécessaire de veiller à l'adéquation entre les effets de défaillance considérés au cours de l'analyse et les causes d'autres modes de défaillance envisagés.

- Effets de la défaillance (colonnes 5 et 6)

De la même façon que le groupe de travail s'est attaché à identifier les causes potentielles de défaillance, il doit examiner les conséquences de cette défaillance, au niveau du composant lui-même tout d'abord (colonne 5) puis au niveau du système global (colonne 6).

- Moyens de détection (colonne7)

Pour le mode de défaillance envisagé, le groupe de travail examine et consigne ensuite les moyens prévus pour détecter ce mode de défaillance.

- Dispositifs de remplacement (colonne 8)

Toutes les dispositions prises, par exemple au niveau de la conception de l'installation, en vue de prévenir ou atténuer l'effet du mode de défaillance doivent alors être examinées. Cette étape, dont les résultats sont consignés en colonne 8, vise d'une certaine façon à caractériser le comportement du système lorsqu'un de ces composants est affecté par un mode de défaillance.

- Evaluation de la criticité (colonnes 9 et 10)

Les colonnes 9 et 10 permettent de consigner les évaluations réalisées par le groupe de travail de la probabilité du mode de défaillance (P) et de la gravité associée à ses conséquences (G). Cette approche permet de mesurer l'influence des barrières de sécurité mises en place et de juger de la pertinence d'envisager de nouvelles barrières au regard du risque présenté. En pratique, il est parfois difficile de disposer de données précises et fiables pour procéder de manière fine à cette évaluation. On pourra alors se référer utilement à des échelles de cotations à plusieurs niveaux de probabilité et de gravité, semblable à celles présentées au paragraphe 3.3.3.1. Rappelons que les échelles de gravité et probabilité quels que soient les formats finalement retenus, doivent êtres présentés et acceptées en début d'analyse.

II.5.6 Outils de l'AMDEC

II.5.6.1 Tableau de cotation des modes de défaillance

Cotation	Gravité (G)	Fréquence (F)	Détection (D)
1	Inexistant	Faible	A l'œil nu
3	Désagrément	Moyenne	Par un examen simple
5	Hors norme	Fréquent	Par un examen détaillé
8	Dangereux	Très fréquent	Par une analyse
10	Mortel	Tous le temps	Indétectable

Tableau II.3 : Tableau de cotation des modes de défaillance

NPR = GxFxD.

II.5.6.2 Feuille d'analyse

AMDEC Produit/Processus														
Produit/Processus: Fiche technique : de travail :					Responsable : Date :						Seuil : Groupe			
Fonction ou Processus	Mode de défaillance	Causes	Effets	Mesures préventives/ Moyens de détection	G	F	D	NPR	Actions correctives (Responsable, délai, etc.)	Résultats des actions				
										Actions prises	G	F	D	NPR

Tableau II.4 : Feuille d'analyse

II.5.7 Limites et avantages

L'AMDEC s'avère très efficace lorsqu'elle est mise en œuvre pour l'analyse de défaillances simples d'éléments conduisant à la défaillance globale du système. De par son caractère systématique et sa maille d'étude généralement fine, elle constitue un outil précieux pour

l'identification de défaillances potentielles et les moyens d'en limiter les effets ou d'en prévenir l'occurrence. Comme elle consiste à examiner chaque mode de défaillance, ses causes et ses effets pour les différents états de fonctionnement du système, l'AMDEC permet d'identifier les modes communs de défaillances pouvant affecter le système étudié. Les modes communs de défaillances correspondent à des événements qui de par leur nature ou la dépendance de certains composants provoquent simultanément des états de panne sur plusieurs composants du système. Les pertes d'utilités ou des agressions externes majeures constituent généralement des modes communs de défaillance. Dans le cas de systèmes particulièrement complexes comptant un grand nombre de composants, l'AMDEC peut être très difficile à mener et particulièrement fastidieuse compte tenu du volume important d'informations à traiter. Cette difficulté est décuplée lorsque le système considéré comporte de nombreux états de fonctionnement. Par ailleurs, l'AMDEC considère des défaillances simples et peut être utilement complété, selon les besoins de l'analyse, par des méthodes dédiées à l'étude de défaillances multiples comme l'analyse par arbre des défaillances par exemple [3].

II.6 Méthode d'analyse par arbre de défaillances

L'analyse par arbre des défaillances fut historiquement la première méthode mise au point en vue de procéder à un examen systématique des risques. Elle a été élaborée au début des années 1960 par la compagnie américaine Bell Téléphone et fut expérimentée pour l'évaluation de la sécurité des systèmes de tir de missiles. Visant à déterminer l'enchaînement et les combinaisons d'évènements pouvant conduire à un événement redouté pris comme référence, l'analyse par arbre des défaillances est maintenant appliquée dans de nombreux domaines tels que l'aéronautique, le nucléaire, l'industrie chimique... Elle est aussi utilisée pour analyser à posteriori les causes d'accidents qui se sont produits. Dans ces cas, l'événement redouté final est généralement connu car observé. On parle alors d'analyse par arbre des causes, l'objectif principal étant de déterminer les causes réelles qui ont conduit à l'accident.

II.6.1 Principe

L'analyse par arbre de défaillances est une méthode de type déductif. En effet, il s'agit, à partir d'un événement redouté défini a priori, de déterminer les enchaînements d'évènements ou combinaisons d'évènements pouvant finalement conduire à cet événement. Cette analyse

permet de remonter de causes en causes jusqu'aux évènements de base susceptibles d'être à l'origine de l'événement redouté. Les évènements de base correspondent généralement à des [1]:

- Évènements élémentaires qui sont suffisamment connus et décrits par ailleurs pour qu'il ne soit pas utile d'en rechercher les causes. Ainsi, leur probabilité d'occurrence est également connue.
- Évènements ne pouvant êtres considérés comme élémentaires mais dont les causes ne seront pas développées faute d'intérêt.
- Évènements dont les causes seront développés ultérieurement au gré d'une nouvelle analyse par exemple.
- Évènements survenant normalement et de manière récurrente dans le fonctionnement du procédé ou de l'installation.
- Quelle que soit la nature des éléments de base identifiés, l'analyse par arbre des défaillances est fondée sur les principes suivants :
  - Ces évènements sont indépendants.
  - Ils ne seront pas décomposés en éléments plus simples faute de renseignements, d'intérêt ou bien parce que cela est impossible.
  - Leur fréquence ou leur probabilité d'occurrence peut être évaluée.

Ainsi, l'analyse par arbre des défaillances permet d'identifier les successions et les combinaisons d'évènements qui conduisent des évènements de base jusqu'à l'événement indésirable retenu. Les liens entre les différents évènements identifiés sont réalisés grâce à des portes logiques (de type « ET » et « OU » par exemple). Cette méthode utilise une symbolique graphique particulière qui permet de présenter les résultats dans une structure arborescente. A l'aide de règles mathématiques et statistiques, il est alors théoriquement possible d'évaluer la probabilité d'occurrence de l'événement final à partir des probabilités des évènements de base identifiés. L'analyse par arbre des défaillances d'un événement redouté peut se décomposer en trois étapes successives :

- Définition de l'événement redouté (ER) étudié.
- Elaboration de l'arbre.
- Exploitation de l'arbre.

Il convient d'ajouter à ces étapes, une étape préliminaire de connaissance du système.

II.6.2 Les objectifs

Les objectifs sont résumés en quatre points [6] :

- La recherche des événements élémentaires, ou leurs combinaisons qui conduisent à **un** ER.
- La représentation graphique des liaisons entre les événements. Remarquons qu'il existe une représentation de la logique de défaillance du système pour chaque ER. Ce qui implique qu'il y aura autant d'arbres de défaillances à construire que d'ER retenus.
- Analyse qualitative cette analyse permet de déterminer les faiblesses du système. Elle est faite dans le but de proposer des modifications afin d'améliorer la fiabilité du système. La recherche des éléments le plus critique est fait en déterminant les chemins qui conduisent à un ER. Ces chemins critiques représentent des scénarios qui sont analysés en fonction des différentes modifications qu'il est possible d'apporter au système. L'analyse des scénarios qui conduisent à un ER est faite à partir des arbres de défaillances, il est alors possible de disposer des "barrières de sécurité" pour éviter les incidents.
- Enfin, il est possible d'évaluer la probabilité d'apparition de l'ER connaissant la probabilité des événements élémentaires. C'est l'analyse quantitative qui permet de déterminer d'une manière quantitative les caractéristiques de fiabilité du système étudié. L'objectif est en particulier de définir la probabilité d'occurrence des divers événements analysés. Les calculs reposent sur : les équations logiques tirées de la structure de l'arbre de défaillance et des probabilités d'occurrence des événements élémentaires.

II.6.3 Définitions

L'arbre de défaillance est une représentation graphique de type arbre généalogique. Il représente une démarche d'analyse d'événement. L'arbre de défaillance est construit en recherchant l'ensemble des événements élémentaires, ou les combinaisons d'événements, qui conduisent à un Evénement Redouté.

L'objectif est de suivre une logique déductive en partant d'un Evénement Redouté pour déterminer de manière exhaustive l'ensemble de ses causes jusqu'aux plus élémentaires.

II.6.3.1 Définitions des évènements

- Événement redouté

L'événement redouté est l'événement indésirable pour lequel nous faisons l'étude de toutes les causes qui y conduisent. Cet événement est unique pour un arbre de défaillance et se trouve au "sommet" de l'arbre [1].

Avant de commencer la décomposition qui permet d'explorer toutes les combinaisons d'événements conduisant à l'événement redouté, il faut défini avec précision cet événement ainsi que le contexte de son apparition.

L'événement redouté est représenté par un rectangle au sommet de l'arbre comme par exemple l'explosion du réservoir de carburant d'un véhicule.

- Événements intermédiaires

Les événements intermédiaires sont des événements à définir comme l'événement redouté. La différence avec l'événement redouté est qu'ils sont des causes pour d'autres événements. Par exemple c'est la combinaison d'événements intermédiaires qui conduit à l'événement redouté. Un événement intermédiaire est représenté par un rectangle comme l'événement redouté. Dans notre exemple c'est la combinaison d'une fuite de carburant avec d'autres événements qui est susceptible de provoquer l'explosion du réservoir.

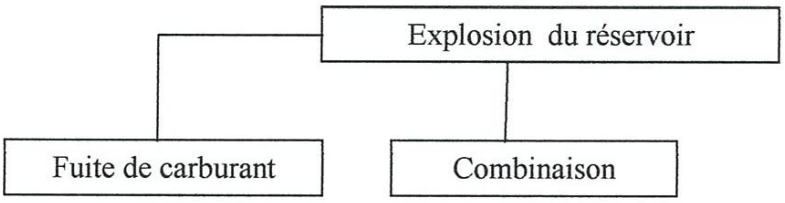


Figure II.2 : Événements intermédiaires

- Événements élémentaires

Les événements élémentaires sont des événements correspondants au niveau le plus détaillé de l'analyse du système. Dans un arbre de défaillance ils représentent les défaillances des composants qui constituent le système étudié.
Pour fixer le niveau de détaille de notre étude, nous considérons en générale que les événements élémentaire coïncident avec la défaillance des composants qui sont réparables ou interchangeables.

Les événements élémentaires sont représentés par des cercles. Dans notre exemple c'est la combinaison de la défaillance Joint percé et Vanne bloquée ouverte qui provoque une fuite de carburant :

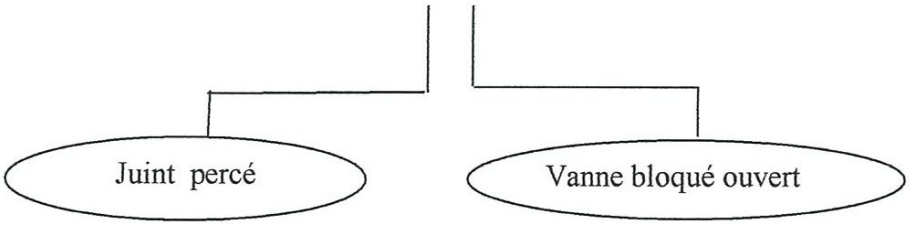


Figure II.3 : Événements élémentaires

- Résumé de la symbolique des événements

Il existe d'autre type d'événements défini par la norme leurs symboles ainsi que leurs signification sont répertoriés dans le tableau suivant.

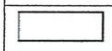
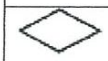
Symbole	Nom	Signification
	Rectangle	Evénement redouté ou événement intermédiaire
	Cercle	Evénement intermédiaire
	Losange	Evénement élémentaire non développé
	Double losange	Evénement élémentaire dont le développement est à faire ultérieurement
	Maison	Evénement de base survenant normalement pour le fonctionnement du système

Tableau II.5 : Symboles des évènements

II.6.3.2 Portes logiques

Les portes logiques permettent de représenter la combinaison logique des événements intermédiaires qui sont à l'origine de l'événement décomposé.

A. Porte ET

L'événement G1 ne se produit que si les événements élémentaires d1, d2 et d3 existent simultanément.

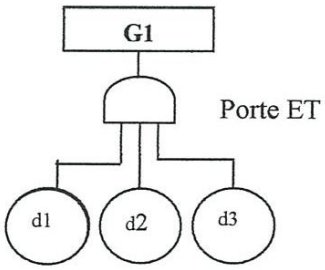


Figure II. 4 : Porte ET

B. Porte OU

L'événement G1 se produit de manière indépendante si l'un ou l'autre des événements élémentaires d1, d2 ou d3 existe.

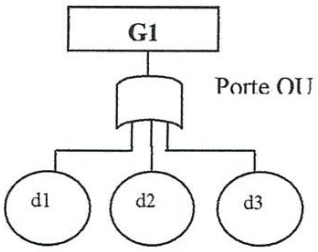


Figure II. 5 : Porte OU

C. Porte R/N

Si R=2 et N=3 alors il suffit que deux des événements élémentaires d1, d2, d3 soient présents pour que l'événement G1 se réalise.

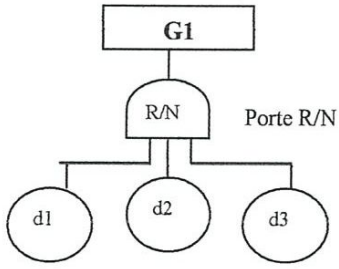


Figure II. 6 : Porte R/N

II.6.3.3 Transfert de sous arbres

Il existe pour les arbres de défaillances une symbolique normalisée qui permet de faire référence à des parties de l'arbre qui se répètent de manière *identique** ou de manière *semblable*$^{+}$ pour éviter de les redéfinir.

L'objectif est de réduire la taille du graphique. Le tableau suivant présente les symboles ainsi que les significations qui sont utilisés.

- Identique : Même structure, mêmes événements.
- Semblable : Même structure mais avec des événements différents.

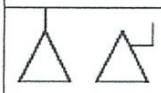
Symbole	Nom	Signification
	Triangle	La partie de l'arbre qui suit le premier symbole se retrouve identique, sans être répétée, à l'endroit indiqué par le second symbole.
	Triangle inversé	La partie de l'arbre qui suit le premier symbole se retrouve semblable mais non identique à l'endroit indiqué par le second symbole

Tableau II.6 : Symboles et significations

II.6.4 Elaboration de l'arbre

La construction de l'arbre des défaillances vise à déterminer les enchaînements d'évènements pouvant conduire à l'événement final retenu. Cette analyse se termine lorsque toutes les causes potentielles correspondent à des évènements élémentaires. L'élaboration de l'arbre des défaillances suit le déroulement suivant [2,8] :

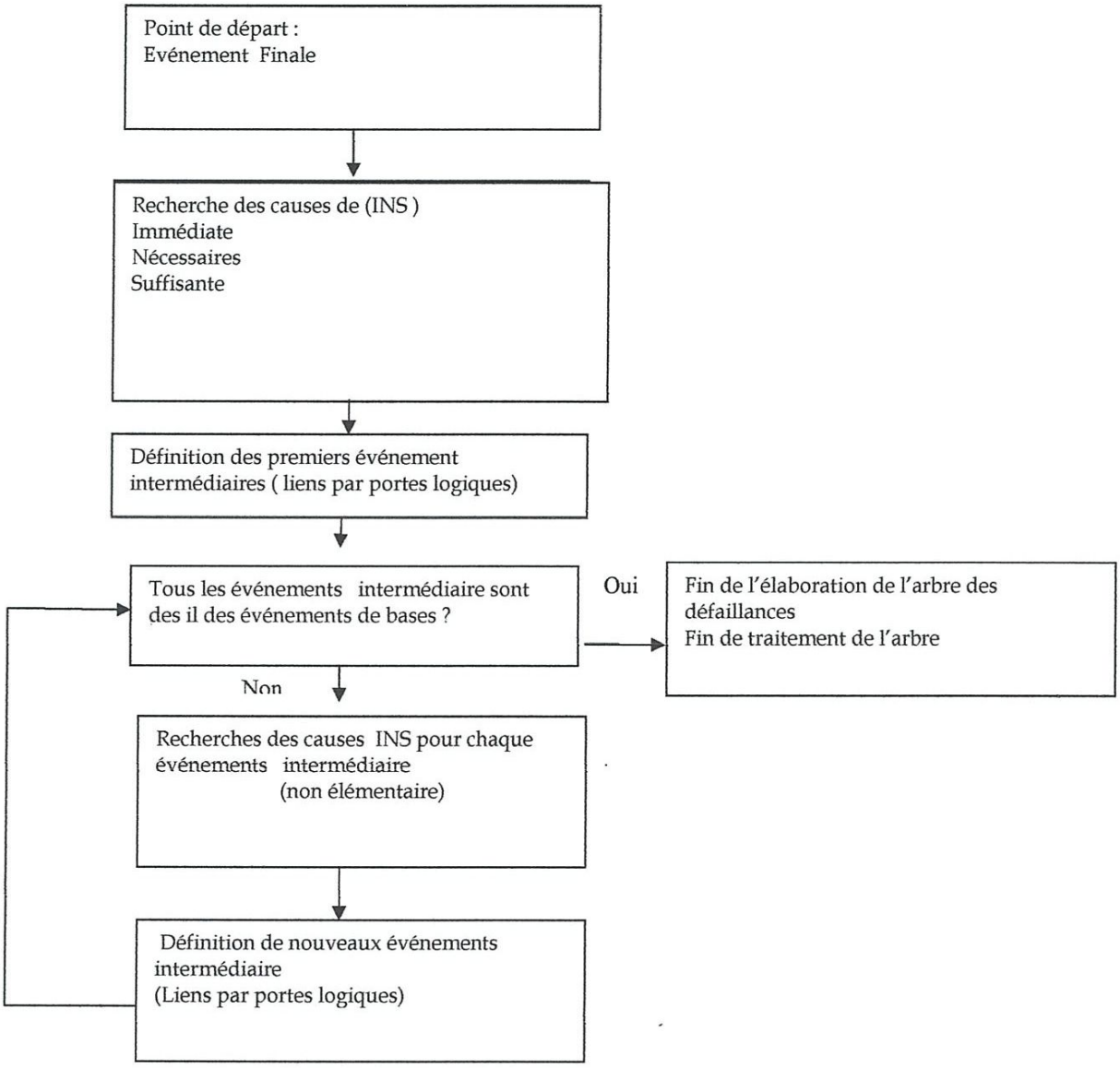


Figure II.7 : Démarche pour l'élaboration d'un arbre des défaillances

La recherche systématique des *causes immédiates, nécessaires et suffisantes (INS)* est donc à la base de la construction de l'arbre. Il s'agit probablement de l'étape la plus délicate et il est souvent utile de procéder à cette construction au sein d'un groupe de travail pluridisciplinaire. De plus, la mise en œuvre préalable d'autres méthodes d'analyse des risques de type inductif facilite grandement la recherche des défaillances pour l'élaboration de l'arbre. Afin de sélectionner les évènements intermédiaires, il est indispensable de procéder pas à pas en prenant garde à bien identifier les causes directes et immédiates de l'événement considéré et se poser la question de savoir si ces causes sont bien nécessaires et suffisantes. Faute de quoi,

l'arbre obtenu pourra être partiellement incomplet voire erroné. Enfin, il est nécessaire de respecter certaines règles supplémentaires à observer durant la construction de l'arbre à savoir :

- Vérifier que le système est cohérent, c'est-à-dire que :
  - La défaillance de tous ses composants entraîne la défaillance du système.
  - Le bon fonctionnement de tous ses composants entraîne le bon fonctionnement du système.
  - Lorsque le système est en panne, le fait de considérer une nouvelle défaillance ne rétablit pas le fonctionnement du système.
  - Lorsque le système fonctionne correctement, la suppression d'une défaillance ne provoque pas la défaillance du système. Il peut en effet arriver qu'une défaillance survenant sur un composant annule les effets d'une défaillance antérieure et permet ainsi le fonctionnement du système. Dans un tel cas de figure (système non cohérent), le deuxième composant doit être supposé, dans l'analyse, en fonctionnement lorsque la première défaillance survient.
- S'assurer que tous les évènements d'entrée d'une porte logique ont bien été identifiés avant d'analyser leurs causes respectives.
- Éviter de connecter directement deux portes logiques.
- Ne sélectionner que les causes antérieures à l'existence de l'événement considéré.

II.6.4.1 Construction d'un arbre de défaillances

La construction de l'arbre de défaillance repose sur l'étude des événements entraînants un événement redouté. Les deux étapes suivantes sont réalisées successivement en partant de l'ER et en allant vers les événements élémentaires.

1. => dans un premier temps définir l'événement redouté (l'événement intermédiaire, ou l'événement élémentaire) analysé en spécifiant précisément ce qu'ils représentent et dans quel contexte il peut apparaître.
2. => puis dans un deuxième temps représenter graphiquement les relations de cause à effet par des portes logiques (ET, OU…) qui permettent de spécifier le type de combinaison entre les événements intermédiaires qui conduisent à l'événement analysé.

Pour pouvoir appliquer cette méthode il est nécessaire de :

- Vérifier que le système a un fonctionnement cohérent.

- Connaître la décomposition fonctionnelle du système.
- Définir les limites du système (le degré de finesse de notre étude dépend des objectifs).
- Connaître la mission du système et son environnement pour déterminer le ou les événements redoutés qui est nécessaire d'étudier.
- Connaître les modes de défaillance des composants [4].

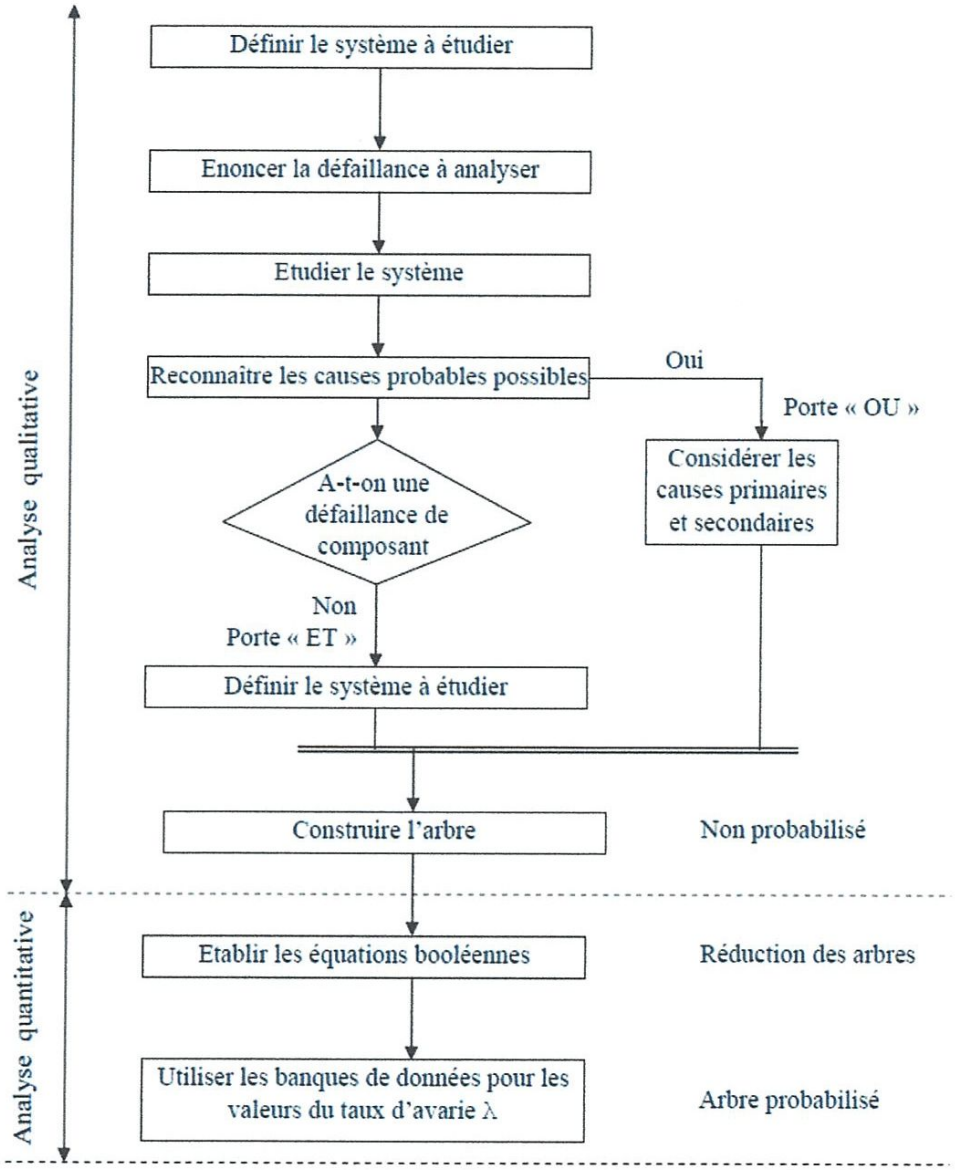


Figure II.8 : Démarche à suivre pour construire un arbre de défaillances.

II.6.4.2 Règles de construction

- Expliciter les faits et noter comment et quand ils se produisent.
  - pour l'événement redouté.

- pour les événements intermédiaires.

➢ Effectuer un classement des événements :

- événement élémentaire représentant la défaillance d'un composant
  - ✓ défaillance première.
  - ✓ défaillance de commande.

➢ Événements intermédiaires provenant d'une défaillance de composant. C'est par exemple un mode de défaillance.

- événements intermédiaires provenant du système indépendamment du composant. C'est par exemple une configuration particulière.

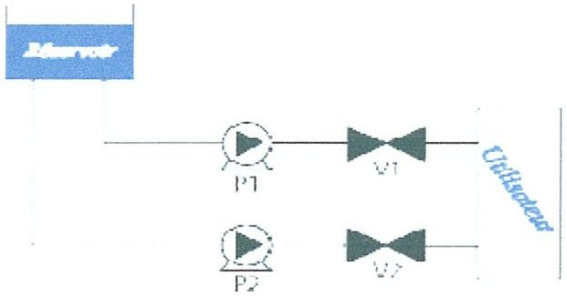
➢ Rechercher les "causes immédiates" de l'apparition de chaque

- événement intermédiaire afin d'éviter l'oubli d'une branche.

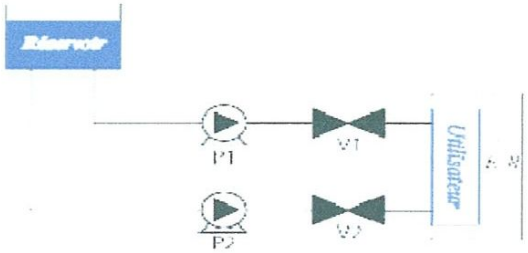
➢ Éviter les connexions directes entre portes : Elles sont en générale dues à une mauvaise compréhension du système ou une analyse trop superficielle.

➢ Supprimer les incohérences : Comme par exemple; un événement qui est à la fois cause et conséquence d'un autre événement.

II.6.4.3 Exemple de construction d'un arbre de défaillance



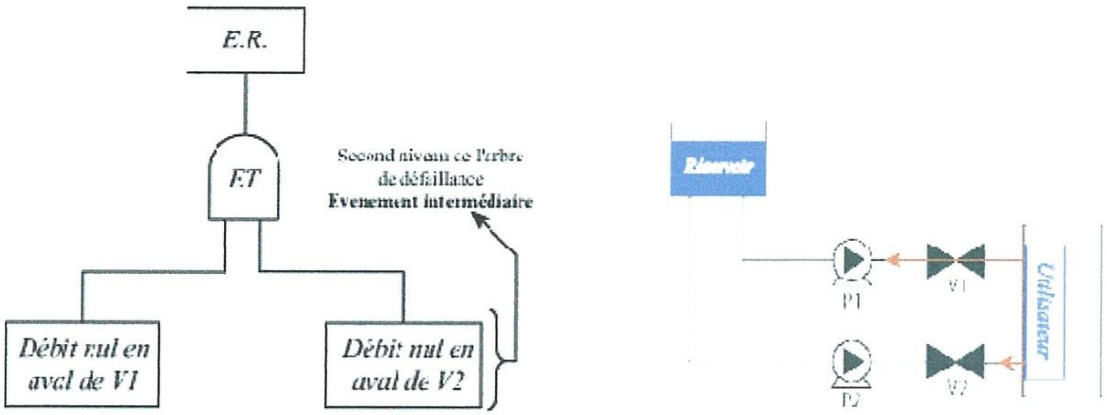
L'événement redouté :



"Le système utilisateur est non alimenté" que l'on nommera ER

Cela se produit si :

"Débit nul en aval de V1" ET "Débit nul en aval de V2"



L'arbre associé est :

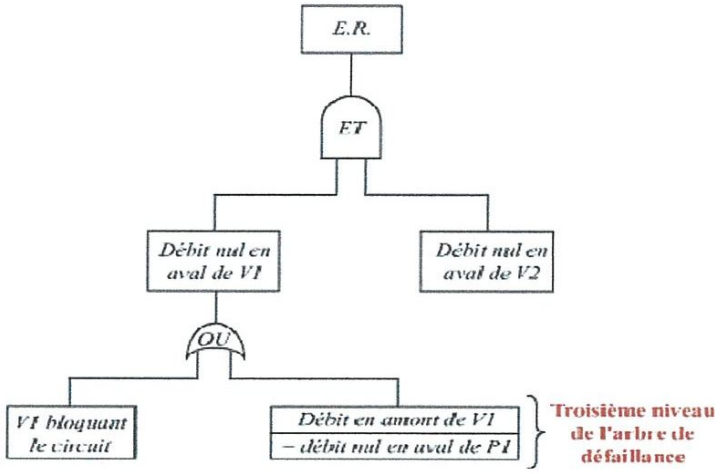


Figure II.9 : L'arbre de défaillance

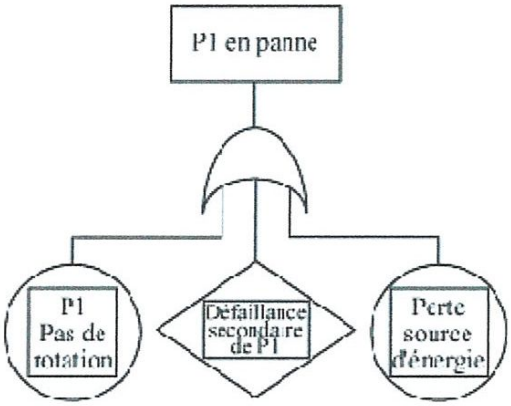


Figure II.10 : Défaillance de commande

1. Défaillance première : Pas de rotation de la pompe.
   - événement élémentaire "P1 - Pas de rotation".

<u>Défaillance première</u> :
Blocage de la vanne en position fermée (un vieillissement).
événement élémentaire :
"V1 bloquée fermée"

<u>Défaillance de commande</u> :
Puisque la vanne est manuelle, cette défaillance serait due à l'opérateur qui n'aurait pas ou mal effectué l'ouverture d'événement élémentaire non développé "opérateur défaillant"

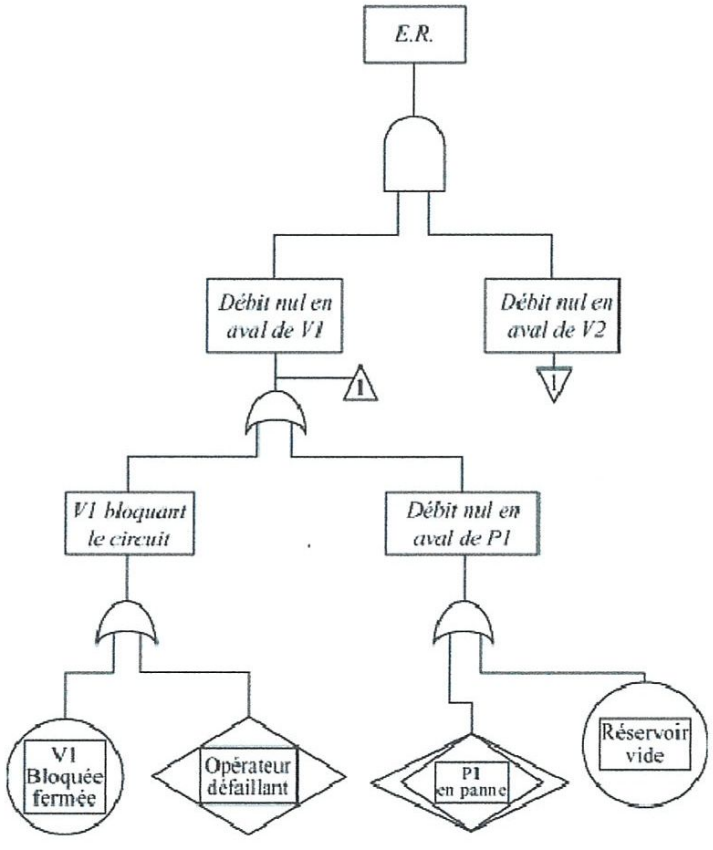


Figure II.11 : Défaillance première

2. Défaillance secondaire : Défaillance due à une cause extérieure ou à une utilisation particulière. Ici un corps étranger qui obstrue la pompe.
   - événement élémentaire non développé "Défaillance secondaire de P1".
3. Défaillance de commande : Puisque la pompe est électrique, cette défaillance serait due à la perte de la source d'énergie.
   - événement élémentaire "Perte source d'énergie".

II.6.5 Exploitation de l'arbre

II.6.5.1 Coupes minimales – Réduction de l'arbre

Une coupe minimale représente la plus petite combinaison d'évènements pouvant conduire à l'événement indésirable ou redouté [2]. On parle parfois également de « chemin critique ». Dans l'exemple suivant:

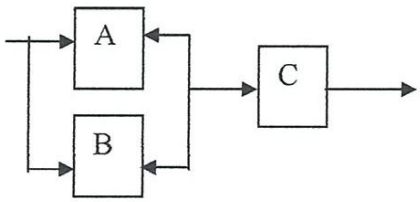


Figure II.12 : Chemin critique

L'occurrence simultanée des évènements A, B et C conduit effectivement à l'événement final. Il ne s'agit cependant pas d'une coupe minimale puisque la combinaison A.B seule peut être à l'origine de l'événement final. La recherche des coupes minimales est effectuée à partir des règles de l'algèbre de BOOLE en considérant que :

- À chaque événement de base correspond une variable booléenne.
- L'événement de sortie d'une porte « ET » est associé au produit des variables booléennes correspondant aux évènements d'entrée.
- L'événement de sortie d'une porte « OU » est associé à la somme des variables booléennes correspondant aux évènements d'entrée. Quelques-unes des principales règles de l'algèbre de BOOLE sont résumées dans le tableau suivant :

La recherche des coupes minimales peut s'avérer fastidieuse pour des arbres de taille importante. Certains outils informatiques permettent heureusement d'automatiser cette démarche. Ces outils démontrent toute leur utilité pour la réduction d'arbres complexes. Leur utilisation ne doit cependant pas faire oublier que la définition précise de l'événement final constitue la première étape en vue de limiter la complexité de l'arbre des défaillances [6].

II.6.5.2 Exploitation qualitative de l'arbre des défaillances

L'exploitation qualitative de l'arbre vise à examiner dans quelle proportion une défaillance correspondant à un événement de base peut se propager dans l'enchaînement des causes jusqu'à l'évènement final. Pour cela, tous les évènements de base sont supposés équiprobables et on étudie le cheminement à travers les portes logiques d'événement ou de combinaisons d'évènements jusqu'à l'événement final. De manière intuitive, une défaillance se propageant à travers le système en ne rencontrant que des portes « OU » est susceptible de conduire très rapidement à l'événement final. A l'inverse, un cheminement s'opérant exclusivement à travers des portes « ET » indique que l'occurrence de l'évènement final à partir de l'événement ou la combinaison d'évènements de base est moins probable et démontre ainsi une meilleure prévention de l'événement final. La définition des coupes minimales permet d'accéder directement aux évènements et combinaisons d'évènements les plus critiques pour le système considéré. Ainsi, plus l'ordre d'une coupe minimale est petit, plus l'occurrence de l'événement final suivant ce chemin critique peut paraître probable. Un moyen de prévenir les évènements indésirables ou redoutés vise à modifier l'arbre des défaillances en vue d'obtenir des coupes minimales d'ordre le plus élevé possible, par l'introduction de portes « ET » par exemple. Cette approche qualitative repose néanmoins sur l'hypothèse relativement forte que les évènements de base sont équiprobables. Il peut cependant arriver qu'une coupe minimale d'ordre 1 corresponde à un événement extrêmement peu probable alors qu'une coupe minimale d'ordre supérieur peut correspondre à des combinaisons d'évènements très probables.

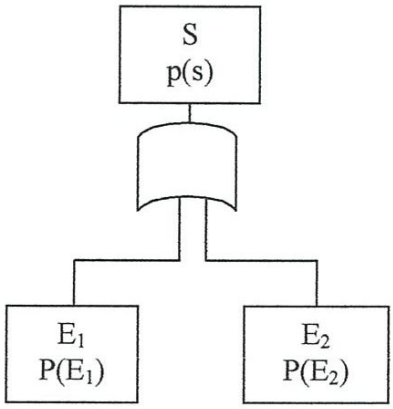
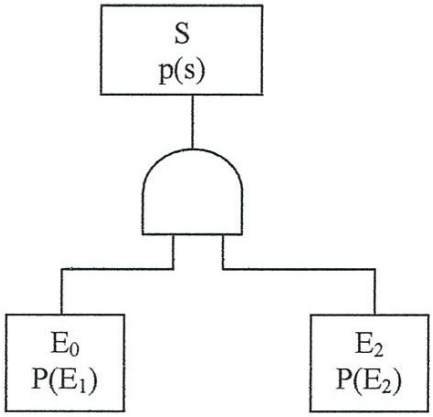
II.6.5.3 Exploitation quantitative de l'arbre de défaillances

L'exploitation quantitative de l'arbre des défaillances vise à estimer, à partir des probabilités d'occurrence des évènements de base, la probabilité d'occurrence de l'événement final ainsi que des évènements intermédiaires. Il ne s'agit pas d'une démarche qui permet d'accéder avec exactitude à la probabilité de chaque évènement. Elle doit être mise en œuvre dans l'optique

de hiérarchiser les différentes causes possibles et de concentrer les efforts en matière de prévention sur les causes les plus vraisemblables. En pratique, il est souvent difficile d'obtenir des valeurs précises de probabilités des évènements de base. En vue de les estimer, il est possible de faire appel à :

- Des bases de données.
- Des jugements d'experts.
- Des essais lorsque cela est possible.
- Au retour d'expérience sur l'installation ou des installations analogues.

À partir des probabilités des évènements de base, il s'agit de remonter dans l'arbre des défaillances en appliquant les règles suivantes :

Porte « OU »	**Porte « ET »**
	
$P(s)= P(E_1) + P(E_2) \_ P(E_1).P(E_2)$ THEOREM DE POINCARRÉ) Lorsque la probabilité des événements de base et faible, il est possible de négligé le double produit $P(E_1)$. $P(E_2)$ et de considérer : $P(S)= P(E_1) + P(E_2)$.	$P(S) = P(E_1). P(E_2)$

À titre d'exemple, appliquons cette démarche à l'arbre réduit présenté en Figure 4, en supposant les probabilités des évènements de base connues :

$P(A) = 10^{-3}$, $P(B) = 10^{-2}$, $P(C) = 10^{-6}$

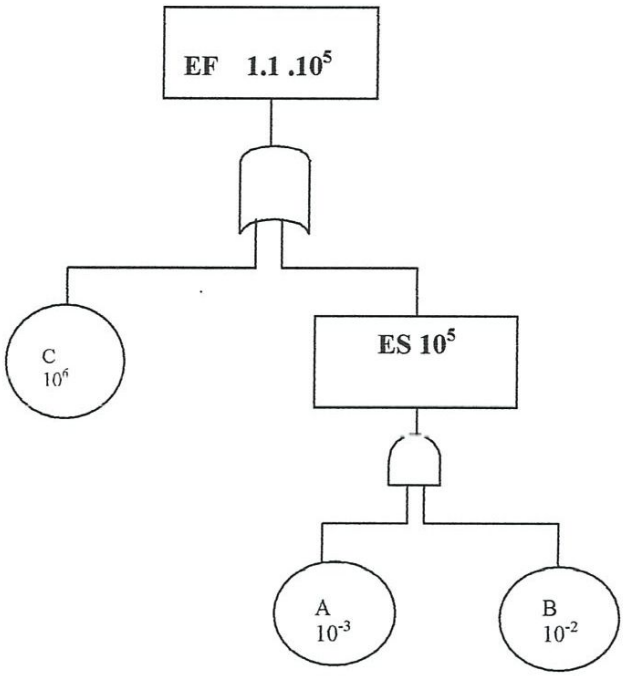


Figure II.14 : Déterminations de la probabilité de l'événement final

Cette exploitation quantitative de l'arbre, au même titre que son exploitation qualitative, ne peut être effectuée qu'à partir d'un arbre réduit. Par ailleurs, notons, que pour des éléments de base de faible probabilité, la probabilité de l'événement final est sensiblement égale à la somme des probabilités affectées aux coupes minimales. Dans l'exemple précédent, nous avons donc: P(EF) = P(C + A.B) = P(C) + P(A).P(B) - P(A).P(B).P(C) (théorème de POINCARRE) d'où P(EF) = P(C) + P(A).P(B) Les logiciels informatiques développés depuis une dizaine d'années permettent de déterminer automatiquement les probabilités tout au long de l'arbre. L'examen des probabilités des évènements intermédiaires conduisant à l'événement final permet de hiérarchiser les priorités de modifications du système en identifiant les causes les plus probables d'un événement indésirable ou final. La réduction de la probabilité de cet événement final peut alors être envisagée de plusieurs manières :

- En supprimant ou réduisant la probabilité d'occurrence des évènements de base.
- En améliorant la fiabilité du système par l'ajout de portes « ET » entre l'événement final et les évènements de base. Les portes « ET » placées au plus proche de l'événement final permettent de traiter un maximum de coupes minimales et le cas échéant, de traiter certaines causes qui n'auraient pas été envisagées.

II.7 Limites et avantages

Le principal avantage de l'analyse par arbre des défaillances est qu'elle permet de considérer des combinaisons d'évènements pouvant conduire in fine à un événement redouté. Cette possibilité permet une bonne adéquation avec l'analyse d'accidents passés qui montre que les accidents majeurs observés résultent le plus souvent de la conjonction de plusieurs évènements qui seuls n'auraient pu entraîner de tels sinistres. Par ailleurs, en visant à l'estimation des probabilités d'occurrence des évènements conduisant à l'événement final, elle permet de disposer de critères pour déterminer les priorités pour la prévention d'accidents potentiels. L'analyse par arbre des défaillances porte sur un événement particulier et son application à tout un système peut s'avérer fastidieuse. En ce sens, il est conseillé de mettre en œuvre au préalable des méthodes inductives d'analyse des risques. Ces outils permettent d'une part d'identifier les évènements les plus graves qui pourront faire l'objet d'une analyse par arbre des défaillances et d'autre part, de faciliter la détermination des causes immédiates, nécessaires et suffisantes au niveau de l'élaboration de l'arbre. Depuis une dizaine d'années, des logiciels informatiques sont commercialisés afin de rendre plus aisée l'application de l'arbre des défaillances. Ces outils se montrent très utiles pour la recherche des coupes minimales, la détermination des probabilités ainsi que pour la présentation graphique des résultats sous forme arborescente [6].

II.8 Méthode de Diagramme de Succès (MDS)

Le diagramme de succès est un modèle permettant de représenter le comportement du système. Ce modèle est caractérisé par un diagramme admettant une entrée E et une sortie S, et des blocs représentant les éléments du système (matériels ou fonctionnels). Les arcs reliant les blocs traduisent les relations entre les différents éléments du système. Par conséquent, la structure du diagramme est naturellement proche de la structure du système. L'ensemble des éléments dont le fonctionnement assure le succès de la mission du système est appelé chemin de succès [1].

II .9 Exemple d'application

Ils permettent de déterminer la probabilité de réussite d'une mission, en mettant en évidence les éléments dont le bon fonctionnement suffit pour assurer cette réussite.

Le système à étudier: 2 lampes assurant l'éclairage d'une machine-outil.

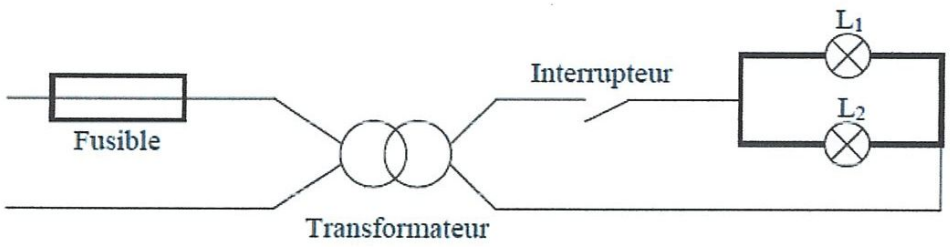


Figure II.15 : Diagramme de fiabilité

Le diagramme de fiabilité correspondant est celui de **la Figure II.16.** Ce digramme montre que tous les éléments doivent fonctionner pour que les lampes L1 et L2 s'allument [8].

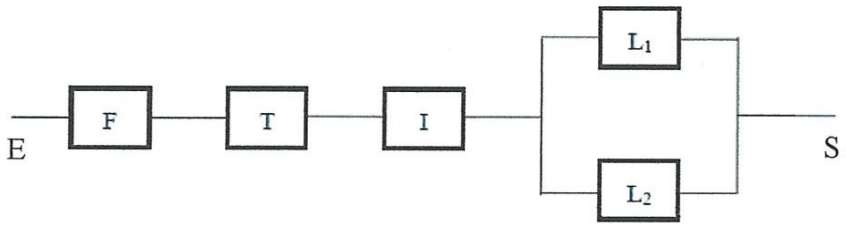


Figure II.16 : Diagramme de fiabilité

- **L'arbre de défaillances probabilisé**

Il correspond à l'analyse quantitative. L'utilisation d'un arbre de causes de défaillance pour évaluer la probabilité d'apparition de l'évènement indésiré repose sur les règles classiques de calcul des probabilités composées à évènements indépendants.

- Porte « ET » : probabilité de « A » et « B » = Pr(A) × Pr(B).
- Porte « OU » : probabilité de « A » ou « B » = Pr(A) + Pr(B) – [Pr(A) × Pr(B)].

Nous allons élaborer l'arbre de défaillances, de l'exemple précédent, suivant le processus mis en place précédemment.

1) Système à étudier: 2 lampes assurant l'éclairage d'une machine-outil.

2) Défaillance à analyser (évènement indésiré): L'obscurité du poste de travail.

3) Les causes probables possibles: Transformateur hors service, panne du secteur, circuit coupé, interrupteur bloqué en position ouverte, fusible hors service, les 2 lampes hors service.

4) Test: La défaillance a-t-elle été provoquée par une défaillance de composant ?
Oui → nous avons donc une porte « OU ».
Les lampes sont H.S, ou les lampes ne sont pas alimentées.
- Si les lampes sont H.S, c'est l'état du système « lampes » qui est en cause: lampe L_1 H.S, et lampe L_2 H.S.
- Les lampes ne sont pas alimentées nous avons: le transformateur H. S, une panne du secteur, le circuit coupé, le fusible H.S, ou l'interrupteur bloqué en position ouverte.

5) Ceci nous donne l'arbre de défaillances ci-dessous (**Figure II.17**).

Lorsque l'analyse qualitative est terminée, nous pouvons quantifier cet arbre de défaillances. L'équation booléenne s'écrire de la façon suivante :

$B = F + G + H + I + J$

$C = D \times E$

$A = B + C$

$A = F + G + H + I + J + (D \times E)$

Connaissant les probabilités d'apparition de chaque élément nous pouvons déterminer la probabilité d'apparition de l'évènement A (**Tableau II.8**) [9].

Elément	**Modes de défaillance**	**Taux de défaillances**
F transformateur	Hors service	10^{-4}
G secteur	Panne	10^{-4}
H circuit	Coupure	10^{-4}
I intérieur	Bloqué ouvert	10^{-4}
J fusible	Hors service	10^{-4}
D lampes L1	Hors service	10^{-4}
E lampes L2	Hors service	10^{-4}

Tableau II.8 : Taux de défaillance

$Pr(A) = Pr(F) + Pr(G) + Pr(H) + Pr(I) + Pr(J) - [Pr(F) \times Pr(G) \times Pr(H) \times Pr(I) \times Pr(J)] + [Pr(D) \times Pr(E)]$.

$= 10\text{-}4 + 10\text{-}4 + 10\text{-}4 + 10\text{-}4 + 10\text{-}4 - [10\text{-}4 \times 10\text{-}4 \times 10\text{-}4 \times 10\text{-}4 \times 10\text{-}4] + [10\text{-}3 \times 10\text{-}3]$.

$Pr(A) = 5\times10\text{-}4 - 10\text{-}20 + 10\text{-}6 = 5{,}01\times10\text{-}4$, car : 10^{-20} peut être négligé.

Ce résultat (taux d'avarie du système $\lambda = 5{,}01\times10\text{-}4$) correspond à la clause (condition) de fiabilité pour notre système.

Remarque

Dans le cas des portes « OU » qui nous donne la probabilité de A ou B = Pr(A) + Pr(B) – [Pr(A) × Pr(B)] nous pouvons négliger le produit [Pr(A) × Pr(B)] si Pr(A) et Pr(B) sont Faibles.

Nous pouvons dans ce cas faire l'approximation suivante :

Pr(A ou B) = Pr(A) + Pr(B).

Dans notre exemple nous aurions :

$Pr(A) = Pr(F) + Pr(G) + Pr(H) + Pr(I) + Pr(J) + [Pr(D) \times Pr(E)] = 5{,}01\times10\text{-}4$.

Ceci nous permet aussi, en appliquant l'algèbre des probabilités, de déterminer le taux de défaillances du système, en utilisant les expressions suivantes [9]:

Porte ET : $\lambda = \lambda_1 \times \lambda_2 \times \lambda_3 \times \ldots\ldots\ldots\ldots \lambda_n$.
Donc :

$$\lambda = \prod_{i=1}^{n} \lambda_i$$

Porte OU : $\lambda = \lambda_1 + \lambda_2 + \lambda_3 + \ldots\ldots\ldots\ldots \lambda_n$.
Donc :

$$\lambda = \sum_{i=1}^{n} \lambda_i$$

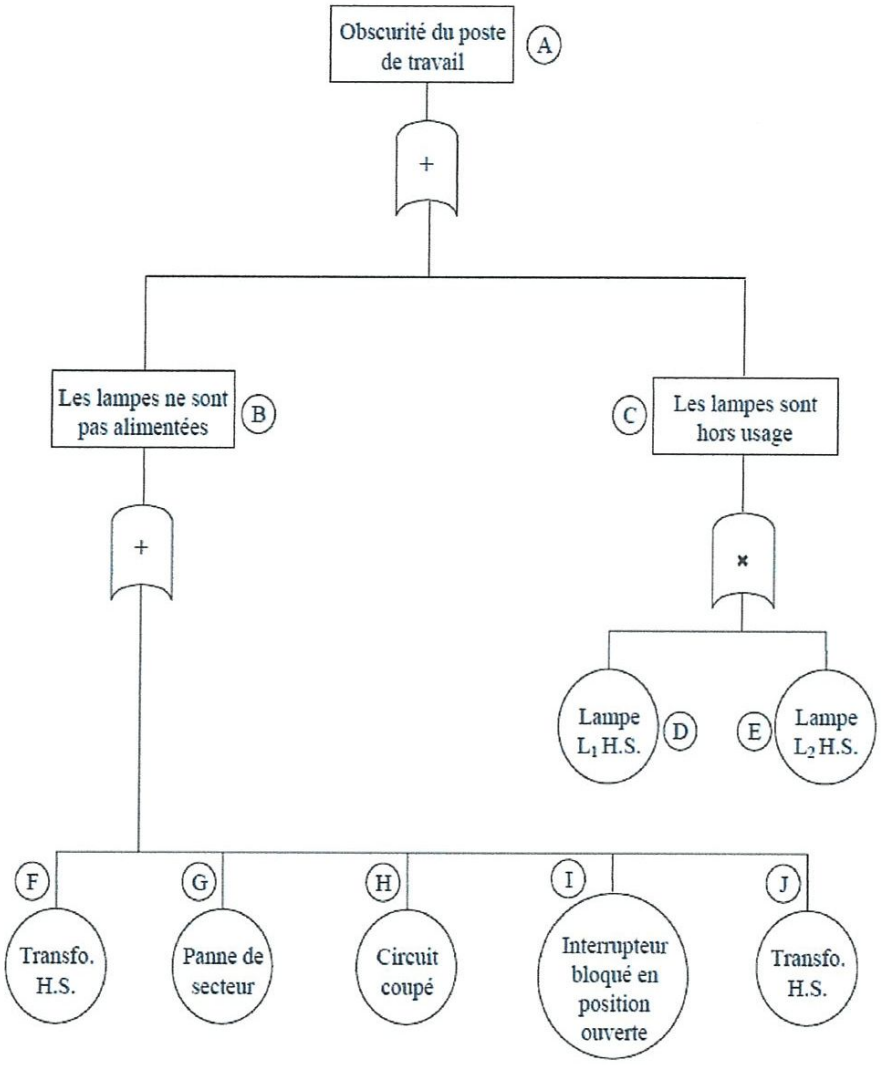


Figure II.17 : Arbre de défaillances

II.10 Conclusion

On a décrit les principales méthodes d'analyse de la sûreté de fonctionnement. Parmi ces méthodes la méthode de L' AMDEC, du diagramme de succès (MDS), et la méthode des arbres de défaillance. Qui feront l'objet d'une application dans le chapitre suivant.

Chapitre 3

Application au système de régulation des réservoirs

III.1 Introduction

Dans le chapitre précédent, nous avons présenté la méthode des arbres de défaillances. Cette méthode est appliquer a travers d'un système industrielle pour la recherche des scénarios redoutés. On traite tout d'abord la notion de coupe minimale, après le système choisi qui est le système de régulation des deux réservoirs.

III.2 Coupe minimale

Une coupe est une combinaison ou un sous-ensemble d'éléments dont la panne entraîne la panne du système.

Une coupe minimale est une coupe ne contenant aucune autre coupe.

La recherche des coupes minimales est un outil clef dans l'étude de la sûreté de fonctionnement d'un système.

En effet, elle permet d'un point de vue qualitatif:

- D'identifier les points faibles du système.
- De repérer les redondances inutiles.
- D'évaluer l'influence d'un élément [1].

Exemple 3.1

Soit le système suivant **Figure III.1** destiné à réguler le niveau d'un fluide dans une cuve. Il se compose de deux vannes (V1 et V2) et de 2 détecteurs de niveau (DH et DTH). Les détecteurs ont un taux de fiabilité de $\lambda = 10^{-3}\ h^{-1}$, les rendant insensible à un niveau haut. Les vannes ont un taux de fiabilité de $\lambda = 10^{-3}\ h^{-1}$, les faisant passer (ou rester) dans un état ouvert. La construction et le traitement de l'arbre de défaillance et faite par le logiciel SimTree [9].

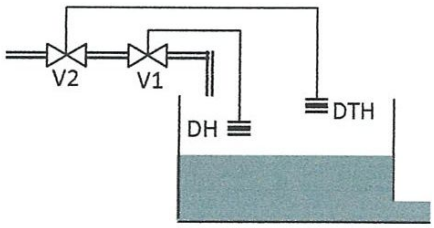


Figure III.1: Régulation de niveau d'un fluide dans une cuve

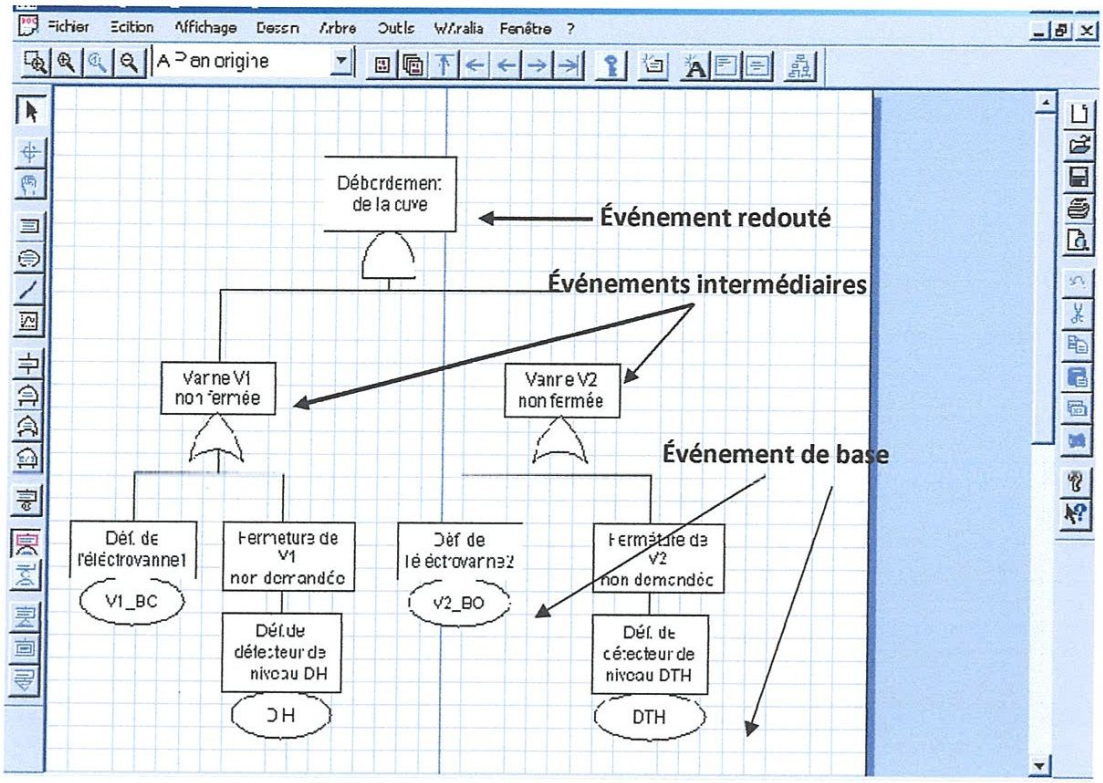


Figure III.2: Arbre des causes du système

La phase qualitative de la méthode MAC mène à l'expression logique caractérisant l'événement redouté. Dans le cas de l'exemple décrit par la **Figure III.2**, l'expression logique associée au débordement de la cuve est définie par la relation (1.1).

$$S=(V1 + DH)\,(V2 + DTH) \qquad (1.1)$$

$$S=V1.V2 + V1.DH + V2.DH + V2.DTH$$

Donc il y a 4 coupes minimales d'ordre 2. La probabilité de l'événement redouté est calculée à partir des taux de défaillance ou de réparation associés aux événements de base ou élémentaires. Ici pour l'exemple précédent est : à 100h, la probabilité est de $3.28585.10^{-2}$ [9].

III.3 Le système de régulation des réservoirs

III.3.1 Présentation

Le cas d'étude est basé sur un système de régulation du volume de deux réservoirs (voir **Figure III.3**). Il est constitué d'un calculateur, de deux pompes, de trois électrovannes (tout ou rien), de deux capteurs de volume et des deux réservoirs

électrovannes (tout ou rien), de deux capteurs de volume et des deux réservoirs régulés (Réservoir 1, Réservoir 2) et d'un troisième réservoir de vidange. Les deux réservoirs régulés alimentent des utilisateurs selon un besoin prédéfini (fonction du temps).

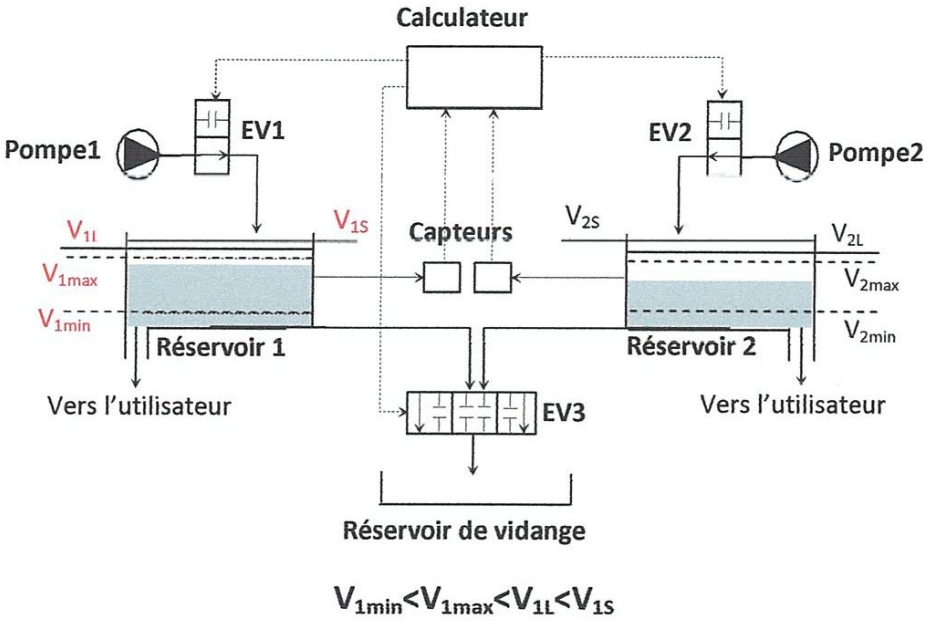


Figure III.3: Système de régulation des réservoirs

Le volume dans chaque réservoir (1 ou 2) doit rester dans un intervalle donné [V_{imin}, V_{imax}]. Le contrôle s'opère à l'aide du calculateur qui décide, selon la valeur du volume (délivrée par le capteur), d'approvisionner (ou non) le réservoir en question en alimentant (ou non) l'électrovanne concernée.

Pour chaque réservoir, on distingue donc deux phases de fonctionnement selon que l'électrovanne alimentant ce réservoir est ouverte ou fermée :

- Une phase de conjonction lorsque l'électrovanne est ouverte. Le volume dans le réservoir est croissant durant cette phase, et cela quel que soit la valeur du débit de sortie vers l'utilisateur (le débit d'alimentation de l'électrovanne est bien supérieur, par hypothèse, au débit de sortie).
- Une phase de disjonction lorsque l'électrovanne est fermée. Le volume dans le réservoir est par conséquent décroissant.

La loi de contrôle du calculateur pour chaque réservoir est telle que lorsque le volume dépasse la limite supérieure de commande V_{imax} pendant la phase de conjonction,

alors le calculateur commande la fermeture de l'électrovanne. Lorsque le volume devient inférieur à V_{imin} (limite inférieure de commande) durant la phase de disjonction, alors le calculateur commande à l'ouverture de cette électrovanne et on change par conséquent de phase de fonctionnement.

Ce système doit assurer l'approvisionnement des utilisateurs tout en évitant le débordement de l'un des réservoirs. Une troisième électrovanne de secours est prévue pour cet effet. Elle est partagée entre les deux réservoirs et assure leur vidange quand ils débordent.

Elle ne peut être utilisée que par un seul réservoir à la fois. Quand le volume dans l'un des réservoirs dépasse la limite supérieure de sécurité (V_{iL}), alors le calculateur commande l'ouverture de cette électrovanne du côté du réservoir qui risque de déborder, jusqu'à ce que le volume devienne inférieur à V_{imin}. En effet, le débit de vidange de l'électrovanne de secours étant supérieur aux débits des pompes 1 et 2, le volume ne peut que décroître pendant la phase de vidange du réservoir concerné.

Nous supposons que seules les électrovannes et les pompes peuvent subir des défaillances. Les électrovannes 1 et 2 (prévues pour l'alimentation des réservoirs) peuvent être bloquées en ouverture, en cas de défaillance de l'électrovanne 3 (de secours), elle est mise hors service. Est la défaillance des pompes 1et 2 [10].

III.4 Modélisations le cas d'étude par la méthode d'arbre de défaillance

III.4.1 Etude qualitative

Le modèle complet du cas d'étude par la méthode d'arbre de défaillance est représenté par le schéma suivant (La construction et le traitement de l'arbre de défaillance et faite par le logiciel SimTree):

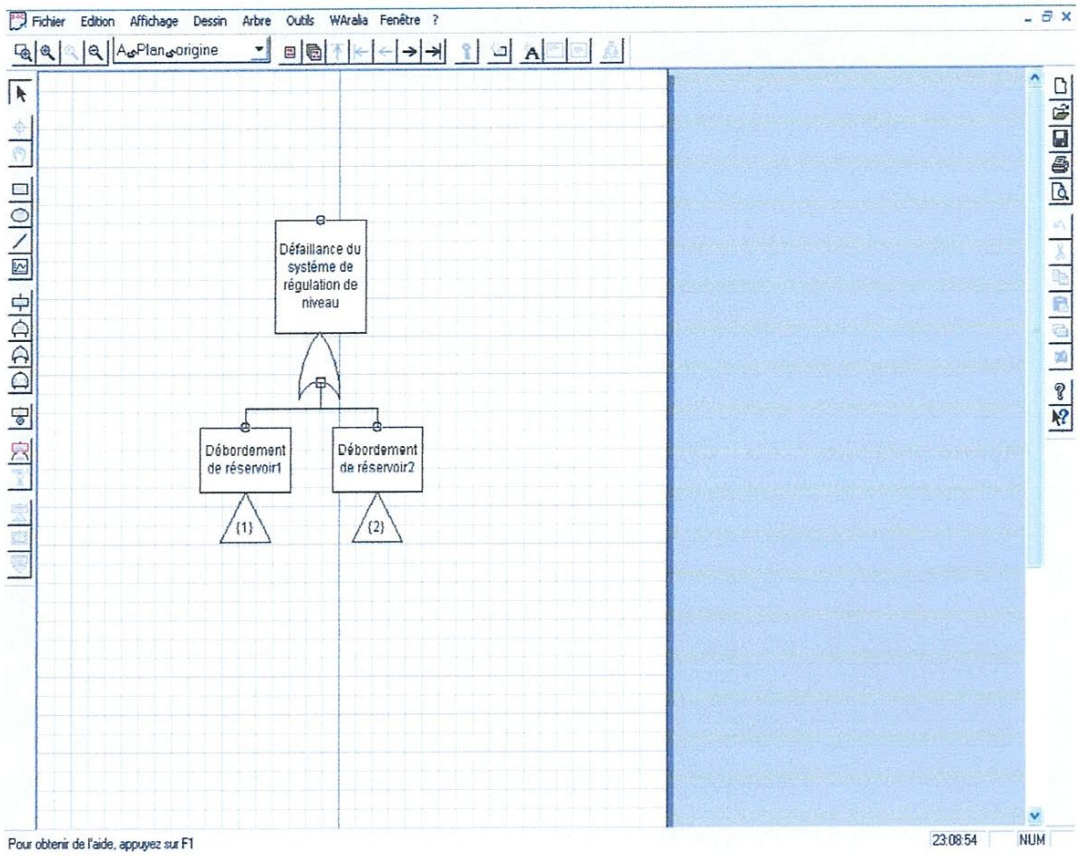


Figure III.4: L'arbre de défaillance du cas d'étude

Ou les triangles 1 et 2 Sont des renvoi dans un nouveau plan, lorsqu'on appuis sur le bouton droit de la souri sur le renvoi1 on trouve le modèle du débordement du réservoir1 (**Figure III.5**).

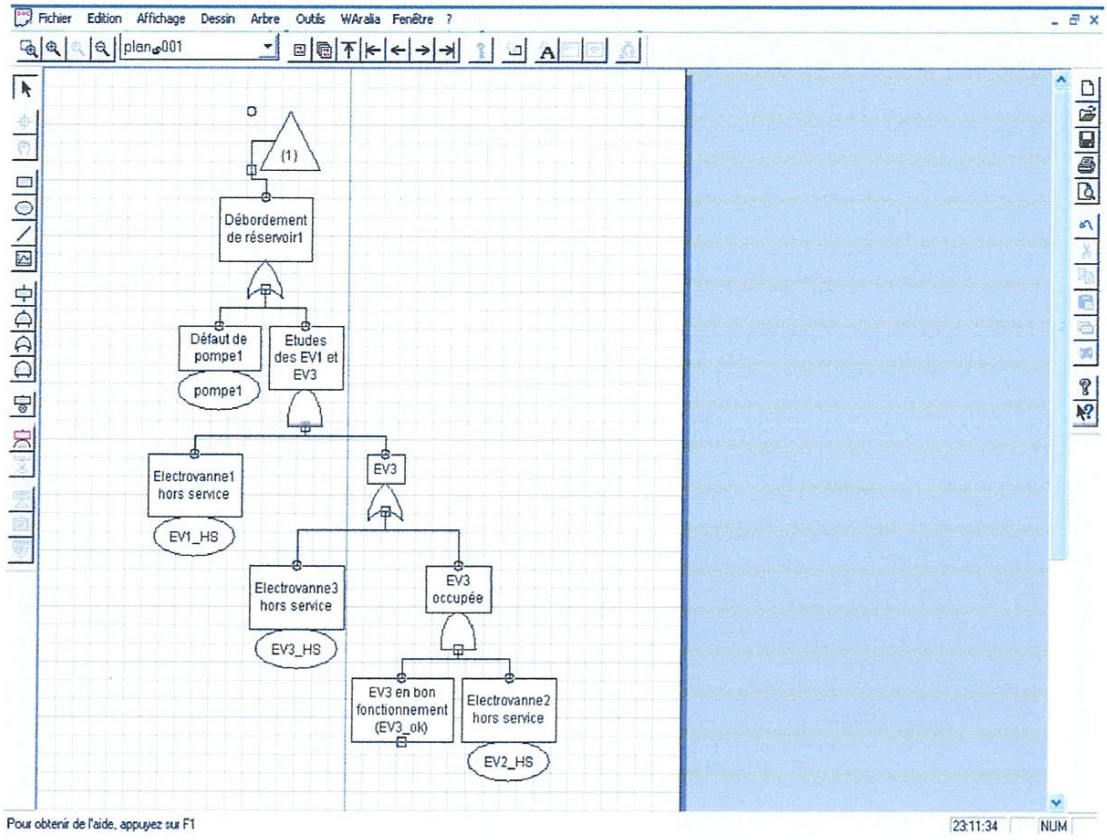


Figure III.5: Arbre de défaillance du réservoir1

Et lorsqu'on appuis sur le bouton droit de la souri sur le renvoi 2 on trouve le modèle du débordement du réservoir2 (**Figure III.6**)

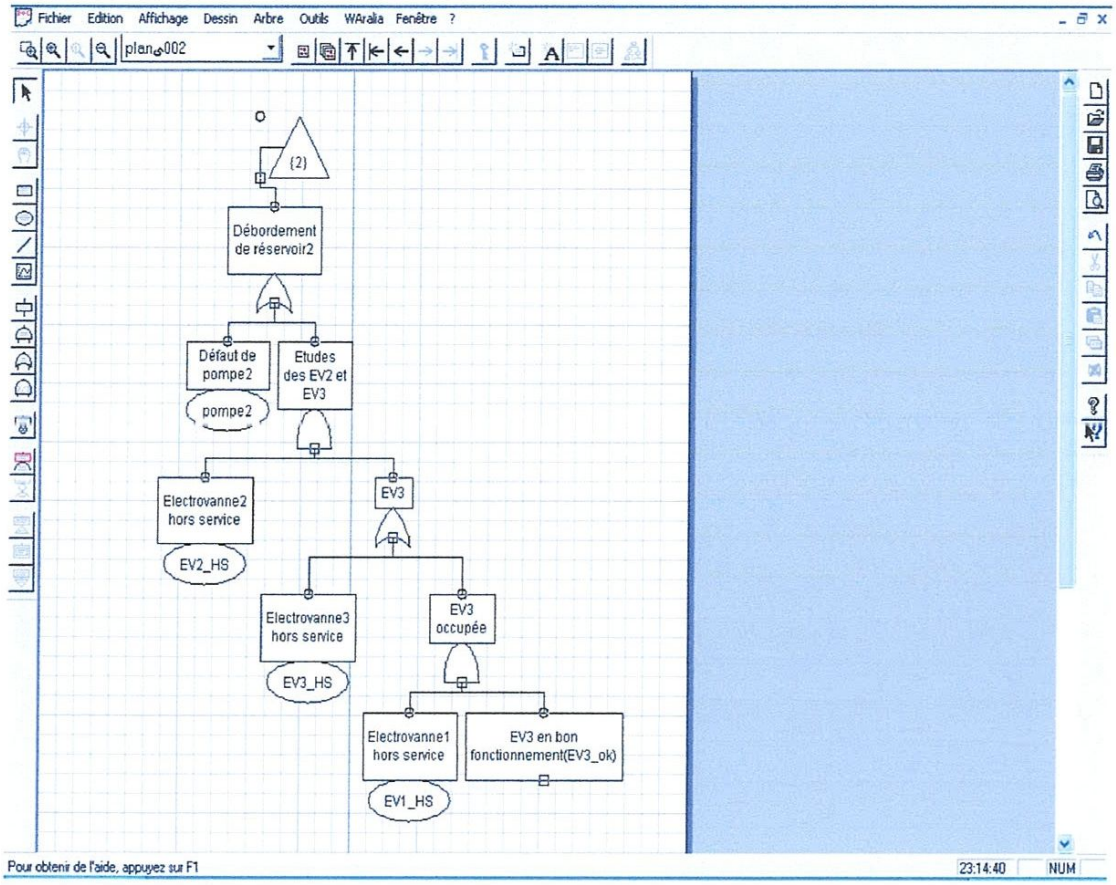


Figure III.6: Arbre de défaillance du réservoir2

Pour calculer les coupes du débordement du réservoir 1 et 2 et du système complet on suit les étapes suivant (**Figure III.7**) :

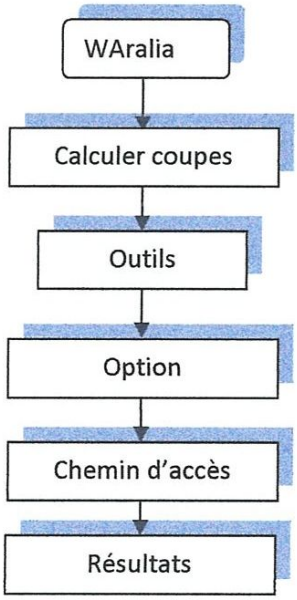


Figure III.7: Les étapes à suivre pour calculer les coupes minimales du système par le logiciel Sim tree

Par exemple pour le réservoir 1 est représenté par la figure suivante (même chose pour le réservoir 2 et le système complet):

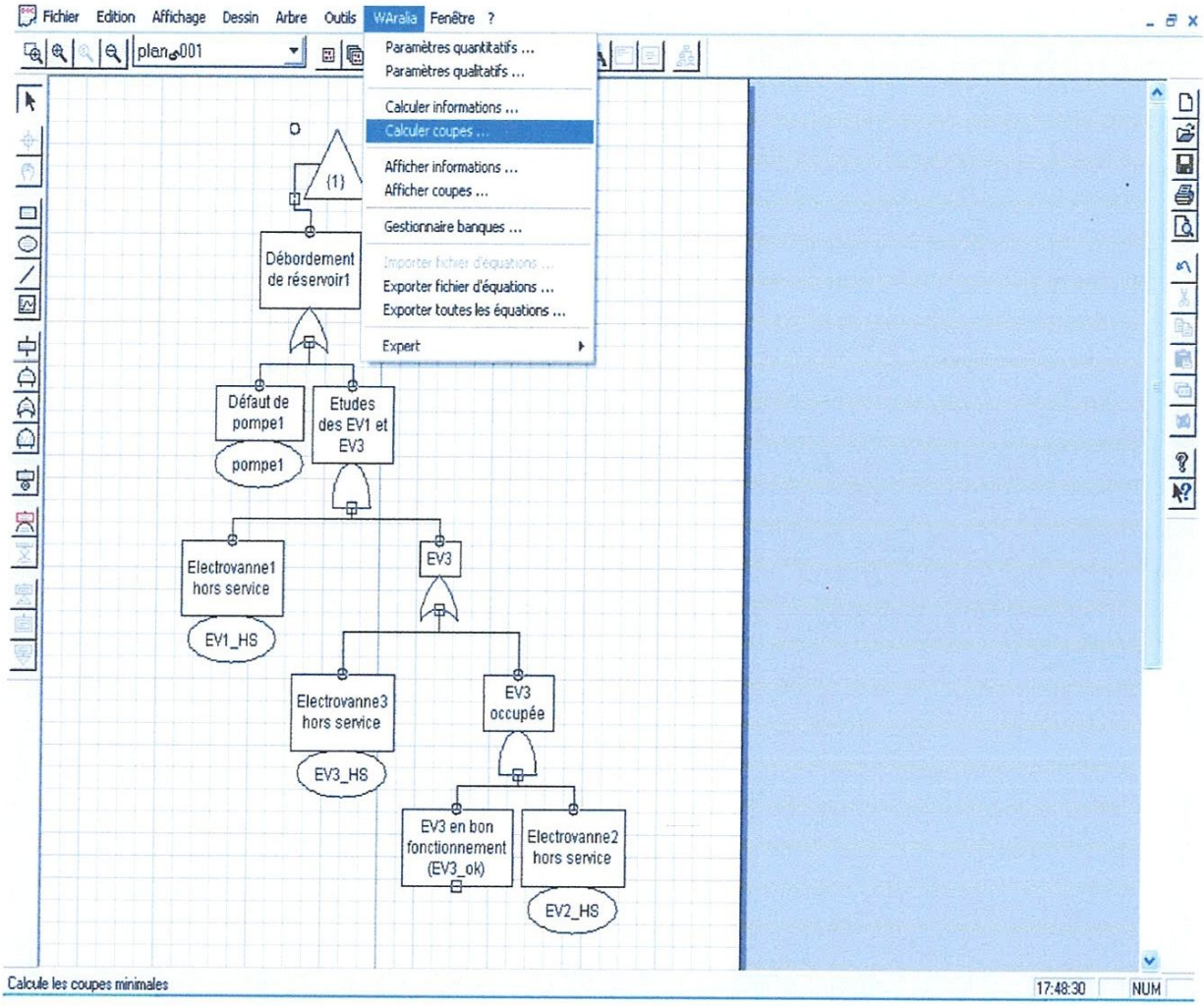


Figure III.8: Les étapes à suivre pour calculer les coupes minimales

III.4.2 Etude quantitative

L'étude quantitative est la probabilité du débordement du système de régulation de niveau des deux réservoirs.

Elément	le taux de réparation μ (S)	Le taux de défaillance λ (Lambda) (S^{-1})
Electrovanne1	0,045	0,43
Electrovanne 2	0,045	0,43
Electrovanne 3	0,045	0,43
Pompe1	0,045	0,43
Pompe2	0,045	0,43

Tableau III.1: Taux de réparation est taux de défaillance des éléments du système

Pour simplifier le calcul de la probabilité de débordement des deux réservoirs, on fait la simplification suivante :

- **Pour le réservoir 1**

SYMBOLE	SIGNIFICATION
A_1	EV1_HS
A_2	EV2_HS
A_3	EV3_HS
A_4	EV3_OK
A_5	EV3
A_6	Défaut P1
A_7	Défaut P2

Tableau III.2: Signification des éléments

L'équation booléenne s'écrire de la façon suivante:

G=H.M

G=EV2_HS.EV3_ok

$G=A_2.A_4$

E=G + F

E=EV3_HS+EV3_occupée

$E=A_3 + A_4$

C=E.D

C=EV1_HS.EV3

$C=A_1.A_5$

$E=F+G$

E=EV3_HS+EV2_HS.EV3_ok

$E=A_3+A_2.A_4$

C=E.D

C=EV1_HS. (EV3_HS+EV2_HS.EV3_ok)

$C=A_1.(A_3+A_2\,A_4)$

C=EV1_HS.EV3_HS+EV1_HS.EV2_HS.EV3_ok

$C=A_1.A_3+A_1.A_2.A_4$

$Pr(c)=Pr(A_1).Pr(A_3)+Pr(A_1).Pr(A_2).Pr(A_4)$

A=B + C

$A=A_6+A_1.A_3+A_1.A_2.A4$

$Pr(A)=Pr(pompe1)+Pr(C)$

$Pr(A)=Pr(A_6)+Pr(C)$

$Pr(A)=Pr(A_6)+Pr(A_1).Pr(A_3)+Pr(A_1).Pr(A_2).Pr(A_4)$

Pr (A)= 0,43 + 0,43. 0,43 + 0,43. 0,43

Pr (A)=0.799

On trouve la probabilité de débordement de réservoir 1 :

$Pr(R_1)=0.799$

Pour la coupe minimale du réservoir 1

$S1=A_6+A_1A_3+A_1A_2A4$

L'ensemble des coupes minimales menant à l'événement redouté (débordement du réservoir 1) décrit par l'arbre de défaillance du renvoi 1 (**Figure III.5**) est :

$S1=A_6+A_1A_3+A_1A_2A_4$

On remarque bien qu'il y a trois coupes minimales l'une d'ordre 1 et l'autre d'ordre 2 et l'autre d'ordre 3.

A partir de cet arbre de défaillance (**Figure III.5**), on trouve ainsi les trois situations critiques (défaut de pompe 1 ou électrovannes 1 et 3 hors service ou électrovanne 1 et 2 hors service et électrovanne 3 occupée à vidanger le réservoir 2).

1er scénarios pour le débordement du réservoir1:

S_1= {défaut_P1 $\vee$ EV1_HS $\wedge$EV3_HS $\vee$ EV1_HS $\wedge$EV2_HS $\wedge$ EV3_occupé}

- **Pour le réservoir 2**

L'équation booléenne s'écrire de la façon suivante :

G=H .M

G=EV1_HS.EV3_ok

$G=A_1.A_4$

E=G + F

E=EV3_HS+EV3_occupée

$E=A_3 + A_4$

C=E.D

C=EV2_HS.EV3

$C=A_2.A_5$

E=F + G

E=EV3_HS+EV1_HS.EV3_ok

$E=A_3 + A_1.A_4$

C=E.D

C=EV2_HS. (EV3_HS+EV1_HS.EV3_ok)

$C=A_2. (A_3 + A_1.A_4)$

C=EV2_HS.EV3_HS+EV2_HS.EV1_HS.EV3_ok

$C=A_2.A_3 + A_2.A_1.A_4$

$Pr (C)=Pr (A_2).Pr (A_3) + Pr (A_2).Pr (A_1)$

A=B+C

Pr (A)=Pr (pompe2) +Pr (C)

$Pr(A)=Pr(A_7) + Pr(C)$

$Pr(A)=Pr(A_7) + Pr(A_2).Pr(A_3) + Pr(A_2).Pr(A_1).Pr(A_4)$

$Pr(A)= 0,43 + 0,43.\ 0,43 + 0,43.\ 0,43$

$Pr(A)=0.799$

Donc la probabilité de débordement du réservoir 2 est :

$Pr(R_2)=0.799$

La coupe minimale du réservoir2 :

$S2= A_7 + A_2 A_3 + A_2 A_1 A_4$

L'ensemble des coupes minimales menant à l'événement redouté (débordement du réservoir 2) décrit par l'arbre de défaillance du renvoi 2 (**Figure III.6**) est :

$S2= A_7 + A_2 A_3 + A_2 A_1 A_4$

On remarque bien qu'il y a trois coupes minimales l'une d'ordre 1 et l'autre d'ordre 2 et l'autre d'ordre 3.

A partir de cet arbre de défaillance (**Figure III.6**), on trouve ainsi les trois situations critiques (défaut de pompe 2 ou électrovannes 2 et 3 hors service ou électrovanne 2 et 1 hors service et électrovanne 3 occupée à vidanger le réservoir 1).

$2^{ème}$ scénarios pour le débordement du réservoir2:

$S_2=$ {défaut_P2 $\vee$ EV2_HS $\wedge$EV3_HS $\vee$ EV2_HS $\wedge$EV1_HS $\wedge$ EV3_occupée}

- **Pour le système de régulation de niveau des deux réservoirs**

Probabilité de débordement du système complet :

$Pr(Sys)=Pr(R_1) + Pr(R_2)$

$Pr(Sys) = 0.799+0.799$

$Pr(Sys) = 1.598$

La coupe minimale du système complet:

$S3 = S1 + S2$

$S3 = (A_6 + A_1 A_3 + A_1 A_2 A_4) + (A_7 + A_2 A_3 + A_2 A_1 A_4)$

$= A_6 + A_1 A_3 + A_1 A_2 A_4 + A_7 + A_2 A_3$

On remarque bien qu'il y a sinq coupes minimales

Le scénario redouté globale pour le débordement du système complet :

S3 = {défaut_P1 $\vee$ EV1_HS $\wedge$EV3_HS $\vee$ EV1_HS $\wedge$EV2_HS $\wedge$ EV3_occupée$\vee$ défaut_P2 $\vee$ EV2_HS $\wedge$EV3_HS}

Donc on trouve le scenario redouté menant au débordement du système complet qui traduit de la façon suivante:

Défaut de la pompe 1 ou défaut de la pompe 2 ou électrovanne 1 et 3 hors service ou électrovannes 2 et 3 hors service ou électrovanne 1 et 2 hors service et électrovanne 3 occupée à vidanger l'une des deux réservoir

III.5 Conclusion

La méthode des arbres de défaillance (AdD) permet de déterminer les scénarios menant à l'occurrence d'un événement redouté tout en décrivant les changements d'états du système à partir d'un état de bon fonctionnement jusqu'à l'occurrence de l'événement redouté en question. Elle permet de regrouper l'ensemble des combinaisons de défaillances menant à cet état sur un seul graphe [1].

Conclusion Générale

Le but de ce travail est l'analyse de la sureté de fonctionnement des systèmes industrielle et plus particulièrement la recherche des scénarios redoutés basé sur la méthode des arbres de défaillance. Nous avons l'appliqué sur le système de régulation des réservoirs.

Ce système utilise une reconfiguration de type partage de ressource. Une électrovanne de secours peut être utilisée par les réservoirs mais une seule à la fois. Ce partage de ressource permet d'optimiser le nombre d'électrovannes de secours, mais pourrait générer des scénarios redoutés inattendus. Ces scénarios trouvés à partir de la méthode des arbres de défaillances basée sur la prise en compte des états de défaillance des composants.

L'analyse quantitative par AdD permet de calculé la probabilité de débordement du système de régulation.
Donc la méthode AdD à pour objectif de déterminer la probabilité et les causes entraînant l'apparition de l'événement redouté et met en évidence les points faibles du système dès sa conception. Elle est largement utilisée dans les études de sûreté de fonctionnement car elle caractérise de façon claire les liens de dépendance, du point de vue du dysfonctionnement, entre les composants d'un système.

Ce travail mérite d'être prolongé, on peut:

- Elaborer une méthode d'analyse quantitative utilisant la simulation de Monte Carlo sur la connaissance des scénarios redoutés (probabilité d'occurrence).