REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITEYAHIA FARES DE MEDEA



Faculté de **T**echnologie

Mémoire de fin d'études de Master

Filière : Hygiène et sécurité industrielle

Spécialité : Hygiène et sécurité industrielle

La sûreté de fonctionnement Méthodes pour maîtriser les risques

---

Présenté par

BENAMOUR BENYOUCEF
CHIKHTOUAMI ABDELFETTAH

Proposé et Dirigé par

RAHMANI AHMED CHERIF

Promotion 2020/2021

Dédicace :

- ***Je dédie ce modeste travail à mes parents, mon père qui me donne des leçons de la vie, et à ma mère pour les conseils précieux, et de m'encourager dans ma vie.***
- ***A ma grande famille mes sœurs et mes frères.***
- ***A ma femme qui m'encouragé de contenue mes études.***
- ***Et à mes filles Soundes , Omaima ,et Sidra à mon fils Mohamed Zakaria et Idris.***

- ***A tous mes amis et surtout le bonhomme*** *CHIKHTOUHAMI ABDELFETAH.*
- ***A tous mes collègues en Hygiène et Sécurité Industrielle.***

Dédicace :

- ***Je dédie ce modeste travail à mes parents, mon père qui me donne des leçons de la vie, et a ma mère pour les conseils précieux, et de m'encourager dans ma vie.***
- ***A mon frère et mes sœurs.***
- ***A tous mes collègues en Hygiène et Sécurité Industrielle.***
- ***A Mon Binôme*** BENAMOUR BENYOUCEF.

Remerciements

D'abord nous remercions dieu, le tout puissant, de nous avoir donné la santé et la volonté pour faire cet humble travail.

***A** mon promoteur de mémoire monsieur le docteur **RAHMANI AHMED CHERIF** à qui j'adresse mes sincères remercîments, ça nous a fait un très grand plaisir qu'Ila accepté de nous encadrer pour ce mémoire, nous apprécions son aide et ses conseils précieux qu'il nous a donné durant notre étude pour la réalisation de ce travail, sa confiance total qui nous permet de travailler ,avec un esprit courageux et confiant, cette confiance était associé avec son soutien et sa gentillesse.*

Votre expérience est un enseignement quotidien pour nous.

Nos remerciements s'adressent ainsi aux :

M. Le président et les membres de jury d'avoir accepté juger et évaluer notre travail.

Mes remerciements s'adressent enfin à tous les collègues de notre promotion pour leurs soutiens et leurs encouragements.

LISTE DES TABLEAUX.

***Tableau1 : Principales** démarches et méthodes de base de Sdf*

***Tableau2:** Analyse des modes de défaillance, de leurs effets et de leur criticité (AMDEC)*

LISTE DES FIGURES.

- ***Figure I.1 :*** *Diagramme de Farmer*
- ***Figure I.2****: Taux de défaillance d'une série de composants : courbe en baignoire****.***
- ***Figure. I.3 :*** *Vie d'un système : évolution dans le temps*
- ***Figure I.4. :*** *Extrait d'un tableau d'AMDE*
- ***Figure I.5.:*** *Un arbre de causes pour le scénario « panne de batterie »*
- ***Figure I.6:*** *Un arbre d'événement pour le scénario « évitement d'un obstacle sur l'autoroute »*
- ***FigureI.7:*** *Un arbre de défaillances : exemple d'une pompe électrique*

Table des matières.

La sûreté de fonctionnement : Méthodes pour maîtriser les risques

Introduction générale : 02

Chapitre I : 04

I. Caractérisation de la sûreté de fonctionnement05

I.1Considérer avec réalisme les entités auxquelles on a affaire05
I.2 Exploiter toutes les connaissances disponibles, rechercher le juste Nécessaire05
I.3 Produire de la confiance partageable grâce à la sûreté de fonctionnement07

Chapitre II: 08

II. Notions fondamentales09

II.1 Sûreté de fonctionnement09
II.2 Risque
II.2.1 Événement redouté10
II.2.2 Fréquence11
II.2.3 Gravité12
II.2.4 Évaluation du risque12
II.3 Fiabilité 14
II.4 Maintenabilité 15
II.5 Disponibilité 16
II.6 Sécurité16

Chapitre III

III. Taux de défaillance, MTBF, MTTF, MUT22

Chapitre IV

IV. Données de fiabilité (ou de maintenabilité) 27

IV.1 Généralités 27
IV.2 Bases de données28
IV.3 Retour d'expérience28

Chapitre V

V. Démarches et méthodes fondamentales d'une approche SdF33

V.1 Présentation des caractéristiques 33
V.2 Analyse préliminaire de risques (APR) 33
V.3 Analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC) 36
V.4 Arbres de causes, d'événement, de défaillances 36
V.5 Graphes d'états. Réseaux de Pétri 41
V.6 Complémentarités entre ces méthodes 43

Chapitre VI

VI. Fiabilités électronique, mécanique, logicielle, humaine 45

VIII. Références bibliographique48

Introduction générale

Introduction générale :

La sûreté de fonctionnement n'est pas un but en soi, mais un moyen ou un ensemble de moyens : des démarches, des méthodes, des outils et un vocabulaire.
Le but qui impose le recours à la sûreté de fonctionnement est plus reconnaissable sous le terme de « maîtrise des risques ».

- Comme il est habituel avec ce type de mots ou d'expressions, « sûreté de fonctionnement désigne à la fois un **ensemble de moyens** et un **ensemble de résultats produits par ces moyens** :

— une forme d'esprit particulière dans la considération portée aux systèmes (en particulier industriels, mais rien ne justifie de se limiter à l'industrie) ; des démarches, méthodes et outils propres à connaître, caractériser et maîtriser les effets des aléas, des pannes, des erreurs... ;
— des caractéristiques des systèmes (produits, services, systèmes de production, installations, etc.), exprimant la conformité dans le temps (constance, fréquence de la conformité) de leurs comportements et actions avec des attentes plus ou moins explicites (on note la proximité de ces notions avec la qualité) : sécurité, fiabilité, disponibilité, maintenabilité, voire invulnérabilité, capabilité, coût global de possession, serviabilité...
Par extension, on parle de la « sûreté de fonctionnement d'un système »comme la caractéristique de ce système qui permet de placer en lui une **confiance justifiée**. C'est d'une simplicité séduisante et trompeuse. La confiance dépend de ce à quoi on accorde de l'importance (innocuité, productivité, qualité... ?) et des valeurs relatives de ces caractéristiques ; elle repose sur un ensemble de **démarches et s'exprime par un ensemble de caractéristiques**, en particulier des disponibilités et de la sécurité. C'est un atout majeur du concept de sûreté de fonctionnement de réunir des approches motivées par la fiabilité, la disponibilité, la maintenabilité et la sécurité, mais c'est un piège de vouloir réduire à une valeur (qui s'appellerait la sûreté de fonctionnement du système) le résultat de ces démarches.

- Les **caractéristiques** pertinentes pour exprimer les fondements de la confiance que l'on place et que l'on veut transmettre dans son système prennent des formes (des noms et des définitions) propres au système dont il s'agit, aux cultures des acteurs concernés et à leurs vocabulaires. Fondamentalement, il s'agit toujours de disponibilité et de sécurité fondées sur des fiabilités et des maintenabilités élémentaires, mais le foisonnement des vocabulaires en usage dans les différentes branches de l'industrie (et encore plus si on élargit au-delà du monde industriel) prouve que chacun a besoin de notions propres adaptées à son contexte.

Par contre, les **démarches et méthodes**, même cachées sous des noms divers et variés, s'avèrent universelles. Plutôt que les caractéristiques, ce sont les méthodes qui seront au cœur de ce premier article. En matière de sûreté de fonctionnement (et pas seulement là), il nous paraît infiniment plus important de comprendre une démarche et un raisonnement, quitte à réinventer le vocabulaire en l'appliquant, que d'apprendre des définitions et des règles, d'utiliser des outils en se laissant guider par eux. Cette dernière pratique, très répandue, conduit malheureusement assez souvent à des conclusions gravement erronées.

La sûreté de fonctionnement n'est que du **bon sens organisé et systématisé**.

S'en éloigner en se laissant conduire par une recette ou une méthode à l'encontre du bon sens est, à coup sûr, s'exposer aux pires dangers d'erreurs graves.

- Maîtriser les risques est une attitude naturelle que chacun pratique ; mettre en œuvre la sûreté de fonctionnement, c'est professionnaliser cette attitude, la systématiser, l'optimiser, l'expliciter.

Concrètement, cela peut se limiter à un état d'esprit spécifique, à quelques questions que l'on se pose systématiquement ; cela peut aussi, à l'inverse, mobiliser des équipes hautement spécialisées en calcul de probabilités, essais, modélisations, analyses, recueil et traitement de données... À chacun son activité, son besoin, ses enjeux, à chacun sa sûreté de fonctionnement, mais le principe en est toujours le même.

Chapitre I

I. Caractérisation de la sûreté de fonctionnement

I. Caractérisation de la sûreté de fonctionnement

La sûreté de fonctionnement (SDF) est peut-être d'abord un état d'esprit avant d'être un ensemble de méthodes. Qu'est-ce qui caractérise cet esprit ?

I.1 Considérer avec réalisme les entités auxquelles on a affaire

Un composant, un sous-système peut tomber en panne.

Un homme peut avoir une activité différente de ce qu'on a voulu lui prescrire.

Les conditions d'environnement peuvent être défavorables, etc.

La sûreté de fonctionnement consiste à ne pas considérer un système uniquement à travers son cahier des charges comme s'il ne devait jamais avoir comme comportements et comme effets que ceux pour lesquels il a été conçu.

I.2 Exploiter toutes les connaissances disponibles, rechercher le juste nécessaire

L'application du principe évoqué au paragraphe 1.1 met donc en présence de nombreuses éventualités d'échecs ou d'accidents.

Il y a l'attitude qui consiste à les ignorer et celle qui consiste à les éliminer totalement. La SDF consiste à remplacer le choix binaire entre ces deux extrêmes par le choix continu entre toutes les positions intermédiaires.

Entre excès de précautions (coûteux, contraignant) et jeu avec le feu (tout va bien jusqu'à la catastrophe), il y a un juste milieu en harmonie avec les grands principes, la politique de son entité (entreprise, association...).

Entre la connaissance déterministe que la panne va toucher tel composant à tel moment et l'ignorance totale (on ne sait pas quelle panne va survenir, ni où, ni quand), il y a des connaissances incomplètes ou incertaines. La sûreté de fonctionnement, loin de les écarter (comme si on ne pouvait rien faire d'une incertitude) les exploite.

Le cas des **composants électroniques** après la Seconde Guerre mondiale est caractéristique, puisqu'il est à l'origine de l'essor évoqué dans l'« historique » : en présence d'un lot de composants « identiques » (fabriqués ensemble), il n'était pas possible (techniquement ou économiquement) de déterminer lesquels allaient tomber en panne et quand.

Par contre, le retour d'expérience montrait une très grande régularité dans le nombre de pannes rapporté au nombre de composants par unité de temps.

Exemple : un **frein de bicyclette** est conçu, fabriqué, installé pour ralentir et arrêter la bicyclette.

Premièrement, la Sdf considère qu'il n'est pas acquis, parce qu'il peut le faire, qu'il va le faire. Il peut ne pas remplir totalement, instantanément, à chaque sollicitation sa fonction.

Deuxièmement, la SdF considère que, à partir du moment où il existe, il va avoir des effets, peut-être sans rapport avec sa fonction.

Normalement, un frein de bicyclette produit de la chaleur, peut faire du bruit, occupe de la place, ajoute du poids à certains endroits. Un freine bicyclette, ce sont des pièces qui pourraient, accidentellement, tomber dans les rayons, des câbles tendus qui pourraient, accidentellement, casser, cingler, blesser, etc. Il y a lieu d'en examiner les conséquences pour faire des choix appropriés.

Une première caractéristique d'une approche sûreté de fonctionnement, c'est le principe de considérer un système pour tout ce qu'il peut être et non seulement pour ce qu'on veut qu'il soit.

- la **sûreté de fonctionnement**.

On note les développements suivants :

— constitution de bases de données de fiabilité ;

— début de normalisation en matière de sûreté de fonctionnement ;

— développement des méthodes d'analyse, de modélisation, de représentation des systèmes complexes ;

— développement de logiciels de calculs ;

— développement de logiciels de modélisation ;

— campagnes d'essais pour recueillir des données de fiabilité ;

— utilisation large ou ciblée de la sûreté de fonctionnement dans la plupart des industries ;

— utilisation de la sûreté de fonctionnement pour maîtriser tout type de risque industriel (et peu à peu des risques juridiques, individuels, financiers, etc.) et non seulement la sécurité ;

— apparition et développement des clauses contractuelles de sûreté de fonctionnement et des exigences légales et réglementaires de sûreté de fonctionnement ;

— besoin croissant de connaissances pointues dans les domaines scientifiques concernés dans les systèmes complexes : systèmes programmés, sciences humaines et sociales.

Aujourd'hui, le terme « **sûreté de fonctionnement** » recouvre l'ensemble des moyens qui permettent de se donner et de transmettre une confiance justifiée dans le succès d'un projet, d'une activité et son innocuité.

Entre une position très prudente consistant à ne pas utiliser ces composants faute de pouvoir éviter les pannes, en les remplaçant à temps par exemple, et une position très risquée consistant à espérer ne pas subir trop de pannes aux mauvais moments, la SdF permet d'évaluer statistiquement le risque pris en fonction des choix d'architecture, de politique de maintenance, etc., mais elle ne le permet que parce qu'il y a une information utile qui est, ici, la loi de probabilité de défaillance des composants en fonction du temps !

I.3 Produire de la confiance partageable grâce à la sûreté de fonctionnement

En vertu du principe évoqué en premier dans le paragraphe 1.1, la sûreté de fonctionnement tend à « tout prévoir » (à ne pas confondre avec « empêcher tout accident »). En vertu du deuxième principielle tend à prendre en compte toute information accessible. Elle offre donc les meilleures garanties possibles que choix et décisions ont pu être faits et pris en toute connaissance de cause.
Il n'y a pas à proprement parler de décisions de SdF. Il y a des décisions techniques, politiques, des choix de conception, d'organisation, d'exploitation, etc., toutes les décisions qui peuvent se prendre dans la vie professionnelle, associative, publique, privée...

La SdF permet de prendre en compte de façon explicite les défaillances, les incertitudes, les aléas... dans toute la mesure, mais seulement dans la mesure, des connaissances qu'on détient à leur Propos.

Ce caractère explicite permet de justifier, de montrer, de discuter, de faire partager la représentation des conséquences (souhaitées et non souhaitées, mais maîtrisées) des décisions que l'on prend ou que l'on veut faire prendre.

Cela souligne aussi le fait qu'il n'y a pas de démarche sûreté de fonctionnement possible s'il n'y a pas de connaissances.

La SdF est toujours totalement dépendant de la connaissance du système étudié et de l'état des sciences concernées.

La recherche de ces informations, en particulier par le retour d'expérience et les essais, est donc indissociable de la SdF.

Chapitre II:

II. Notions fondamentales

II. Notions fondamentales

La démarche, le raisonnement « sûreté de fonctionnement » s'appuient sur quelques notions de base qui se sont précisées au cours de l'évolution (cf. Historique) et qui continuent à s'affiner.
Parcourir ce vocabulaire de base est donc une introduction classique à la sûreté de fonctionnement.
Le lecteur trouvera d'autres définitions importantes dans un glossaire.

II.1 Sûreté de fonctionnement

La sûreté de fonctionnement est souvent définie comme :
— fiabilité, disponibilité, maintenabilité et sécurité ;
— science des défaillances ;
— maintien de la qualité dans le temps.
Toutes ces définitions sont reconnues à divers titres par l'Institut de Sûreté de Fonctionnement (ISDF). Chacune de ces définitions est porteuse de beaucoup du contenu de la SdF, mais chacune est Cependant réductrice, trop étroite.
_ La définition « **fiabilité, maintenabilité, disponibilité et sécurité** » fait donc référence aux définitions de ces termes (§ 2.3 à§ 2.6) et met en avant la cohérence de ces approches. Par contre, si la fiabilité (ou la maintenabilité, la disponibilité et la sécurité) est aussi une performance d'un système, la SdF ne se réduit pas facilement à une performance.
_ La définition « **science des défaillances** » met l'accent sur la prise en compte des défaillances, de leurs causes, de leurs effets et souligne, en parlant de science, l'importance de la connaissance sur les défaillances (causes, effets, mécanismes...) sans laquelle il n'y a pas d'approche SdF. Mais elle est réductrice en ce sens que la SdF prend en compte et traite plus que des défaillances.
En ce qui concerne les événements finaux (les **conséquences**), la SdF ne prend pas en compte que les défaillances dans l'accomplissement des fonctions requises (ce qui serait seulement une approche fiabilité, maintenabilité, disponibilité ou « *dependability* »), mais aussi des événements sans rapport avec le cahier des charges fonctionnel du système (approche orientée sécurité).
En ce qui concerne les événements initiateurs (les **causes**), la SdF ne se limite pas aux défaillances, mais peut permettre de prendre en compte aussi bien des agressions de l'environnement, des action si n'attendues ou interdites des utilisateurs ou des tiers, des phénomènes
aléatoires...
_ La définition « **maintien de la qualité dans le temps** » souligne l'importance de la durée et l'importance de la référence à de exigences (explicites ou non).
Elle a le défaut de laisser supposer qu'une activité SdF se conduit nécessairement dans le cadre d'une démarche qualité, ce qui est faux. C'est le choix – explicable historiquement– de certains

secteurs industriels où la sûreté de fonctionnement est très développée à l'intérieur de l'organisation Qualité, mais n'est pas une nécessité ; d'autres secteurs ont une forte expérience de la sûreté de fonctionnement antérieure à la Qualité au sens moderne incarné par les normes ISO 9 000 et bien d'autres, en particulier une expérience de la sûreté de fonctionnement orientée vers la sécurité.

II.2 Risque

Reformuler en terme de risque les éléments de décision qui relèvent de la prise en compte des dysfonctionnements, des aléas, des erreurs, des agressions de l'extérieur... c'est déjà intégrer l'esprit de la sûreté de fonctionnement.

Utiliser la sûreté de fonctionnement, c'est rechercher et exploiter les informations relatives aux événements non voulus : pannes, agressions, aléas..., les prendre en compte pour des décisions plus fines, plus justes, inspirant plus confiance.

Aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données. On notera que ce concept peut englober la fiabilité, la disponibilité, la maintenabilité, la sécurité, la durabilité... ou des combinaisons de ces aptitudes.

Au sens large, la SdF est considérée comme la science des défaillances et des pannes [2].

Événement redouté évalué en termes de **fréquence** et de **gravité**.

En sûreté de fonctionnement, il s'agit d'identifier les événements in désirables, d'évaluer la fréquence de leurs survenues et de quoi elle dépend, d'évaluer la gravité de leurs survenues et de quoi elle dépend ; de prendre ses décisions en fonction de leurs impacts sur le triplet « événement, fréquence, gravité » qu'on appelle risque.

II.2.1 Événement redouté

On devrait peut-être parler plutôt d'événement incertain, mais comme on n'applique généralement la démarche qu'aux **événements craints**, on a pris l'habitude de parler d'**événement redouté**.

_ Comme on va développer au cours de l'analyse des relations de cause à conséquence, il est très important et parfois délicat d'associer l'événement redouté au système qui le produit.

Il faut bien situer la **frontière** entre ce qui peut produire l'événement redouté (c'est-à-dire ce qui pourrait être modifié pour influer sur la survenue de l'événement) et ce sur quoi peut agir l'événement redouté (c'est-à-dire ce qui pourrait être modifié pour influer sur les conséquences de l'événement redouté).

_ Les événements redoutés d'un système donné, c'est-à-dire d'un «ensemble (de matériels, de logiciels, d'hommes) organisé pour assurer des fonctions données dans des conditions données » sont de **deux types** :

— les écarts aux exigences du cahier des charges, c'est-à-dire ne pas assurer une fonction donnée dans les conditions données ;

— les atteintes à la vie ou la santé, aux biens, à l'environnement, au système lui-même, à quoi que ce soit de précieux causées par un fonctionnement par ailleurs satisfaisant ou par un dysfonctionnement.

Les premiers sont caractéristiques d'une approche « ***fiabilité*** »; ils sont faciles à identifier dès qu'un cahier des charges clair existe.

Les seconds sont caractéristiques d'une approche « **sécurité** » (même sans préjuger de leur gravité) ; on ne peut jamais être certain de les avoir tous identifiés.

II.2.2 Fréquence

C'est l'inverse d'un temps, un nombre d'occurrences par unité de temps.

Derrière cette apparente simplicité se cache une notion pleine de difficultés.

Le temps en question peut s'exprimer en heures, jours ou années.

Encore faut-il préciser si ce sont des jours de calendrier ou des jours ouvrables, des heures sous tension électrique ou des heures de fonctionnement, etc.

Le temps peut aussi s'exprimer en nombre de sollicitations, en distance parcourue, en cycles de température, en tonnes supportées, etc.

Dans une **démarche d'évaluation des risques**, le choix de l'unité est imposé par le modèle qui décrit le plus fidèlement le comportement du système étudié et qui donne la plus grande confiance dans l'extrapolation de l'avenir à partir du passé.

Dans une **démarche d'acceptation de risques**, le choix de l'unité exprime un modèle d'acceptation de risques.

Au cours d'une étude, on est donc amené à combiner des fréquences exprimées relativement à des temps différents (ou in fine à comparer des fréquences issues de modèles physico-chimiques par exemple dans une unité et des critères d'acceptation issus de modèles sociaux exprimés dans une autre).

La **solution simple** consiste généralement à convertir en une unité commune :

— sachant que les circuits électriques sont sous tension en moyenne 72 heures par semaine, on convertit des heures sous tension en temps de calendrier ;

— sachant qu'il circule en moyenne 114 trains par jour sur telle section de voie, on convertit un nombre de circulations en temps de calendrier, etc.

Cette opération est licite... **MAIS** les conclusions de l'étude ne sont valables qu'assorties de l'hypothèse « tant que les circuits restent en moyenne 72 heures par semaine sous tension » ou « tant que le trafic moyen journalier de la ligne est de 114 trains », etc.

Il n'est que trop courant que cette condition soit perdue de vue et que les conclusions de l'étude soient indûment étendues à des systèmes ou des conditions où elles ne sont plus valables.

II.2.3 Gravité

La gravité est la valeur accordée à l'événement. Il est plus parlant, puisque l'on parle d'événements redoutés, de dire « le prix que l'on est prêt à mettre pour éviter l'événement ».

Il faut tout de suite remarquer que la gravité est une ***grandeur subjective***. Elle dépend de l'événement, mais tout autant du point de vue duquel on l'évalue.

Les gravités s'expriment souvent sur des échelles de gravité (usuellement à trois, quatre ou cinq niveaux).

Attention : en général, les gravités ne s'additionnent pas.

Si la fréquence d'un événement complexe (panne totale de la production) se détermine par combinaison des fréquences des causes élémentaires, la gravité ne se calcule pas par combinaison de gravités élémentaires des causes, mais par évaluation des conséquences.

II.2.4 Évaluation du risque

Intuitivement, on admet facilement qu'il y a une **équivalence** entre un événement rare et grave et un événement fréquent et bénin.

— la rupture d'un câble est un événement du système « câble » ; ce n'est pas un événement du système « atelier » ;

— la blessure du manutentionnaire qui a été coupé par la moitié de câble rompu est un événement du système « atelier » et non un événement du système « câble ».

Confondre ces événements conduit à considérer que la seule façon de protéger le manutentionnaire de cet accident est d'empêcher la rupture du câble, ce qui conduit sans doute à supprimer le câble, etc., alors qu'il y a bien d'autres solutions à envisager (éloignement, protection..).

Exemple : la probabilité de rupture d'une pièce mécanique présente généralement de bonnes régularités rapportée au nombre de cycles de charge et décharge (mais pas rapportée au temps de calendrier).

Inversement, des composants électroniques passifs peuvent présente des densités de défaillance stables par unité de temps de calendrier.

Exemple : la fréquence des accidents du travail dans une entreprise présente vraisemblablement du sens en rapportant le nombre d'accidents au nombre d'heures travaillées par exemple, moins vraisemblablement en le rapportant à la consommation électrique ou au nombre de jours de calendrier.

Exemple : l'écrasement d'un ballon par une voiture n'a pas la même gravité pour l'enfant qui jouait avec, pour ses parents, pour l'automobiliste, pour la société...

L'incendie du bâtiment de l'entreprise n'a pas la même gravité pour l'entreprise, son propriétaire, son directeur, ses employés, ses clients, la commune, les riverains, les fournisseurs, l'assureur, etc.

Quand on parle de risque, il faut donc avoir les idées claires sur :

— le système auquel on s'intéresse ;

— les mesures du temps qui sont pertinentes pour représenter le système et pour les décisions à prendre ;

— les points de vue de ceux pour lesquels on produit une évaluation.

Exprimer explicitement et clairement cette équivalence est l'expression d'une échelle de valeurs : c'est un acte de stratégie et non l'expression d'une vérité scientifique.

Décider à combien de jambes cassées équivaut un mort n'a rien d'objectif ; c'est l'expression d'un choix de valeurs de société.

_ Quand la fréquence et la gravité s'expriment en chiffres, il est usuel de faire le produit des deux (qu'on appelle souvent **criticité**, mais ce terme connaît diverses acceptions). On considère alors implicitement que deux risques évalués par la même valeur de ce produit sont également acceptables. Pourquoi pas ?

Il faut toutefois être conscient que cette décision est une décision stratégique lourde et non le simple bon sens.

_ La façon la plus parlante d'exprimer le risque est de placer chaque événement redouté étudié sur un plan dans un repère dont les axes sont la fréquence f et la gravité g. On peut représenter n'importe quel choix d'équivalence de risques en traçant des lignes qui joignent l'ensemble des points qu'on considère également acceptables.

Par exemple, l'hypothèse à propos de la criticité revient à prendre pour lignes iso risques les hyperboles.

Parmi les lignes iso risques, une est particulièrement intéressante: celle qui relie les points à la frontière entre l'acceptable et l'inacceptable.

Son tracé, sa forme, est l'expression très lisible des critères d'acceptation des risques.

Un risque placé au-dessus d'elle doit être réduit pour devenir acceptable :

— soit on en réduit la fréquence, c'est faire de la ***prévention*** ;

— soit on en réduit la gravité, c'est faire de la ***protection***.

Ce **diagramme fréquence-gravité**, aussi appelé diagramme **de Farmer**(figure **1**), est la façon la plus pratique d'illustrer et de communiquer sur le risque, ses trois composantes, ses deux dimensions...

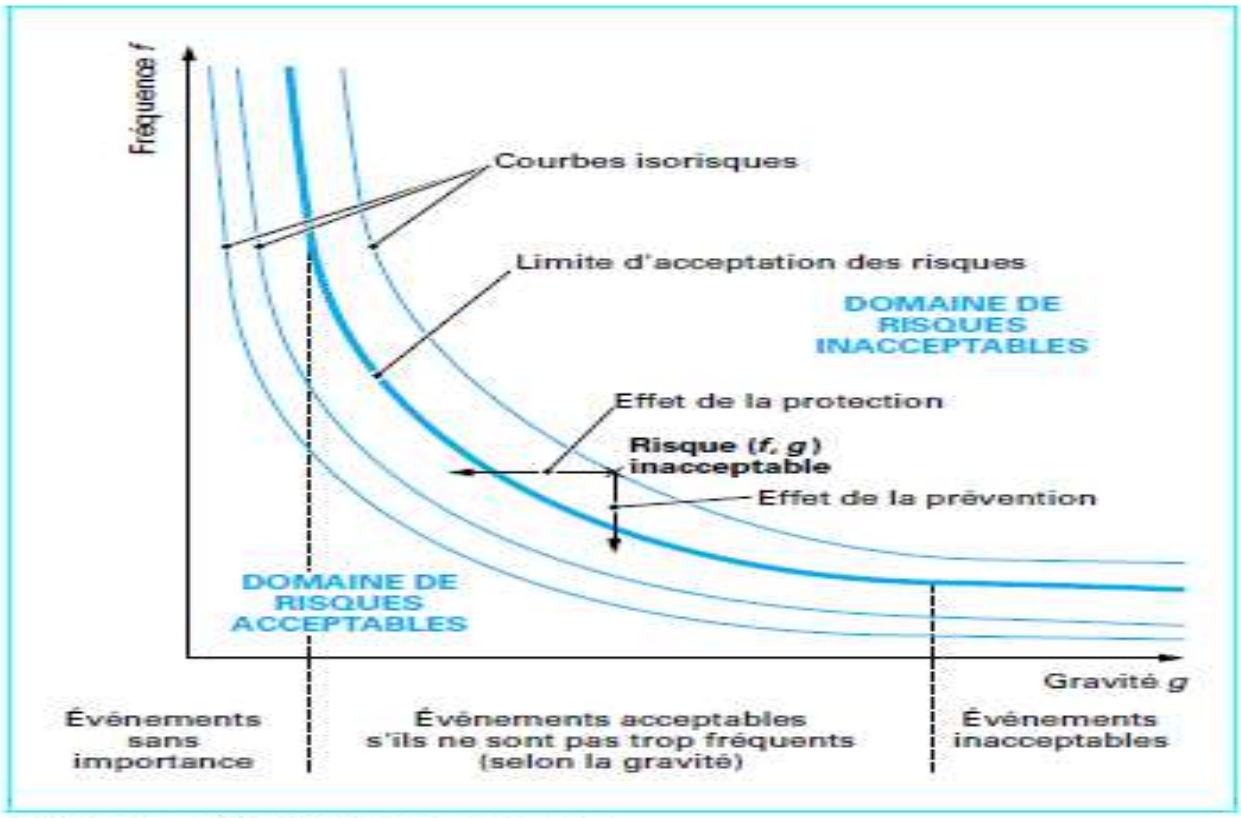


Figure 1 – Diagramme de Farmer

II.3 Fiabilité

La fiabilité est la notion dont la formalisation et l'approfondissement au milieu du siècle fondent une spécialité (la fiabilité ou le calcul de fiabilité et les fiabilistes qui la pratiquent) qui va s'étendre et rejoindre d'autres approches.

La lettre *R* est utilisée souvent pour noter la mesure de la fiabilité parce qu'en anglais (en américain), Fiabilité se dit *Reliability*.

_ « Aptitude » et « entité » sont des mots vagues qui contribuent à ne pas restreindre la définition. En effet, cette définition, tout à fait représentative des définitions les plus couramment admises, définit la fiabilité plutôt comme une caractéristique que comme un ensemble d'activités permettant de conférer cette caractéristique (cf. introduction).

Or, plus cette approche a progressé, plus il est devenu évident que ce qui conditionnait la continuité du service rendu était large ; aussi, ce terme « aptitude » englobe-t-il tout ce qui contribue à la continuité du service rendu.

De même, on s'est aperçu que cette approche était applicable non seulement à des produits, mais aussi à des services, des unités de production, des entreprises, des ateliers, etc. D'où le choix du terme très ouvert « d'entité ».

_ Le reste de la définition, par contre, apporte des précisions :

_ La fiabilité se réfère à une expression de besoins. On ne peut parler de fiabilité qu'après avoir exprimé ce que l'on attend de l'entité considérée.

C'est un point essentiel qui peut se traduire par l'existence de plusieurs fiabilités pour la même entité selon le point de vue auquel on se place ; si plusieurs personnes ont des exigences à l'égard de l'entité, ils ont donc chacun leur notion de fiabilité.

Chacune est légitime ; chaque fois que l'on va parler de la fiabilité de l'entité, il importe de s'assurer que les fonctions requises sont bien identifiées.

_ La fiabilité n'a de sens que dans certaines limites des conditions de fonctionnement de l'entité. Il importe de les préciser.

Personne n'attend la même fiabilité d'un circuit électronique donné dans un environnement protégé des ondes électromagnétiques, des vibrations, des écarts de températures, des écarts de caractéristiques de l'alimentation électrique et à bord d'une locomotive électrique par exemple.

Là aussi, on peut associer à une même entité plusieurs fiabilités correspondant aux mêmes fonctions requises, mais à des conditions d'utilisation différentes.

_ Enfin, ce qui différencie la fiabilité de ses voisines (maintenabilité, disponibilité...) est dans « pendant une durée donnée ».

En effet, la fiabilité est la notion qui caractérise la continuité, l'absence d'interruption du service attendu. La fiabilité, c'est la rareté des défaillances.

_ Le « Petit Robert » estime que le terme est répandu depuis 1962, que son origine remonte au XIIIe siècle et donne comme définition :

— 1. « Aptitude d'un système, d'un matériel à fonctionner sans incidents pendant un temps donné » .

— 2. « Caractère d'une chose, d'une personne fiable ».

Cette définition fait l'économie de souligner lourdement les points essentiels comme notre définition « technique », mais il s'agit bien de la même notion. La sûreté de fonctionnement précise, outille, formalise, systématise des idées et des raisonnements qui sont courants, quoique disponibilité au sens où nous l'entendons et ne soient pas dans les dictionnaires usuels.

2.4 Maintenabilité

La maintenabilité ne se différencie de la fiabilité que sur ce dernier point : elle caractérise la promptitude de reprise du service attendu après interruption.

La maintenabilité, c'est la brièveté des pannes (état dû à une défaillance).

On ne peut s'entendre sur la maintenabilité qu'après avoir explicité les moyens(procédures, outils, organisations...) mis en œuvre pour remettre l'entité en état d'assurer son service. De ce fait, ce n'est a priori pas une grandeur intrinsèque à l'entité. Mais, à conditions d'utilisation données, à moyens de maintenance fixés, c'est une caractéristique de l'entité.

2.5 Disponibilité

La lettre *A* est l'initiale du terme anglo-américain *Availability*.

La disponibilité est une synthèse de la fiabilité et de la maintenabilité ; c'est la proportion du temps passé en état de remplir les fonctions requises dans les conditions données.

L'indisponibilité (son complément) est la proportion du temps passé en panne.

_ Pendant longtemps, et encore dans la majorité des publications, la disponibilité était placée sur le même plan que **la fiabilité et la maintenabilité**. Résultant de « l'addition » de celles-ci, elle représente la proportion du temps où l'entité est apte à rendre le service.

Pour une entité non réparable, elle ne se distinguait pas vraiment de la fiabilité.

Pour une entité réparable, elle était d'autant meilleure que les pannes étaient plus rares (fiabilité) et plus courtes (maintenabilité).

_ De plus en plus, l'intérêt de cette notion apparaît comme une synthèse des notions élémentaires **de fiabilité et de maintenabilité** ,faisant le lien entre ces notions nécessaires aux fiabilistes et la qualité de service qu'elle peut être perçue par un client ou un utilisateur.

La disponibilité résultant, pour un système réparable, en partie de la maintenabilité, la remarque faite au paragraphe 2.4 sur l'importance de la détermination des moyens de maintenance vaut pour la disponibilité.

_ De ce fait, on a vu apparaître des **définitions diverses** de la maintenabilité et de la disponibilité visant à distinguer des notions n'incluant que des caractéristiques propres à l'entité (c'est-à-dire intrinsèques) ou incluant plus ou moins de caractéristiques de l'environnement (essentiellement la maintenance) dans lequel elle sera plongée.

2.6 Sécurité

Nota : « **Sûreté** » est parfois employé dans le sens donné ici plutôt à « Sécurité ».

C'est généralement le cas dans le domaine du nucléaire.

Le sens – large – donné ici à « Sécurité »est plus proche en anglais de *Safety* que de *Security*. Les positions relatives de Sécurité et de Sûreté, en particulier dans les domaines qui utilisent les deux, sont différentes d'un domaine à l'autre et la discussion de ces différentes définitions serait assez longue sans apporter au lecteur d'idées supplémentaires pour s'approprier une démarche SdF. Aussi ce sujet est il évité ; que ceux qui ne se retrouveront pas dans cette brève remarque (et ils seront nombreux pour des raisons diverses et parfois opposées) veuillent bien nous en excuser.

On n'a généralement guère de difficultés en considérant comme équivalent de sécurité *Sicherheit*, *Sicurrezza*, *Seguridad*... et une combinaison plus ou moins englobante de *Safety*, *Security* et *Integrity*.

Un apport essentiel de la SdF est d'intégrer la sécurité aux fiabilités, maintenabilité et disponibilité dans une approche globale.

C'est un apport, parce que cela n'a pas toujours été de soi et que ça ne va toujours pas de soi dans de nombreux domaines.

Pourtant, c'est un progrès, parce que la maîtrise des risques, qu'elle s'exprime par rapport à des objectifs de sécurité ou des objectifs de qualité de service – fondée sur fiabilité, maintenabilité et disponibilité –, agit sur les mêmes décisions.

La sécurité est la notion la plus ancienne dont l'origine se perde dans la nuit des temps.

Les travaux de terminologie de l'ISDF montrent que, contrairement aux trois termes précédents dont les définitions ne souffrent que de différences superficielles, les définitions de la sécurité sont très diverses.

Particularités de la sécurité : les éléments communs qui restent généralement liés à l'idée de sécurité sont :

— les événements redoutés sont graves, très graves ;

— la sécurité, c'est de la confiance justifiée (elle ne peut se réduire à un chiffre).

Puisque l'on envisage les événements les plus graves, on envisage des risques qui ne sont acceptables que si la fréquence est extrêmement basse. Cela a plusieurs conséquences :

— on recherche toutes les possibilités d'accidents graves sans pouvoir négliger ceux qui ont une vraisemblance de se produire très faible ;

— on cherche à évaluer des couples (fréquence-gravité) avec des valeurs infiniment petite/infiniment grande dont la multiplication n'a guère de sens et qui sont extrêmement sensibles aux incertitudes ;

— la détermination de seuils d'acceptation du risque est une démarche difficile et lourde de sens en soi.

_ C'est une particularité forte d'une démarche axée sur la sécurité que le souci d'exhaustivité dans le recensement des événements redoutés.

Il est difficile par l'analyse d'imaginer les combinaisons les plus rares (de pannes, d'erreurs, de données, de conditions extérieures, d'agressions...) qui peuvent conduire à un accident grave.

Il n'est pas acceptable d'attendre que les accidents se soient produits au moins une fois pour les porter sur la liste des scénarios d'accidents possibles.

_ Une autre particularité forte d'une démarche axée sur la sécurité est que le calcul de probabilités présente beaucoup de difficultés et que son utilité est modeste.

En effet, le calcul sur des valeurs extrêmes sollicite des méthodes peu intuitives et l'interprétation des résultats exige beaucoup de rigueur et conduit souvent à des conclusions très imprécises.

Heureusement, en matière de sécurité, on dispose généralement de peu d'historique d'accidents graves.

On doit donc s'appuyer sur des événements moins graves et des modèles de prédiction des accidents graves.

Le calcul de probabilités a un rôle à jouer en matière de sécurité (il est utilisé dans toutes les industries « à risques »), mais, si important qu'il paraisse à cause de l'impression de force laissée par les mathématiques utilisées, il ne peut qu'être un élément modeste parmi d'autres pour construire une confiance justifiée dans l'innocuité d'un système.

_ C'est, enfin, une particularité forte de la sécurité que la détermination des objectifs ou des seuils d'acceptabilité ne dépend pas seulement des responsables du système, mais aussi des pouvoirs Publics et de la société sous différents aspects.

Contrairement aux objectifs de *F, M, D* (Fiabilité, Maintenabilité, Disponibilité), on ne peut traduire en valeur monétaire un accident grave ou un niveau de sécurité sans être réducteur et discutable (et discuté).

De même, le coût d'une mesure de sécurité ne se réduit pas nécessairement à une valeur monétaire. Les mesures de sécurité sont en grande partie des contraintes ou des restrictions acceptées ou imposées à l'activité.

Tout devrait pouvoir, selon des courants de pensée plutôt dominants de nos jours, s'évaluer en valeur monétaire ; toutefois, dans ce cas, il faut s'attendre à ce qu'aucune évaluation ne fasse consensus.

_ Les accidents graves sont considérés par la loi et la société comme inacceptables.

Toute partie impliquée dans une activité « à risques » doit donc déterminer le risque acceptable, ce qui peut être considéré comme un équivalent pratique de l'impossible.

On est donc amené à distinguer le coût d'un accident (condamnation civile à la réparation des dommages), qui peut se multiplier par la fréquence estimée pour évaluer le risque pris, et le niveau de sécurité acceptable, pour les différentes composantes de la société (risque de condamnation pénale pour prise de risque excessive).

Dualité de la sécurité : fiabilité très élevée et exhaustivité des impacts possibles sur le système et en dehors.

Il est plus juste de prendre l'adjectif « sûr » dans ses deux sens : hors de danger et certain de l'être.

Les fiabilistes dès les années 50/60 ont cherché à aligner la définition de la sécurité sur les définitions toutes neuves de la fiabilité, de la maintenabilité, de la disponibilité..., d'où la définition, donnée au début du paragraphe, qui ne rend justice qu'à l'aspect« fiabilité des valeurs extrêmes » de la sécurité.

Contrairement à la fiabilité, la sécurité déborde largement l'entité à propos de laquelle la question se pose.

Il ne s'agit pas seulement du fonctionnement de l'entité, mais des conséquences de son existence et de ses fonctionnements (y compris anormaux, accidentels...).

Il ne s'agit pas seulement du service à rendre, mais des intérêts de tout ce qui peut être touché (survie de l'entité, préservation des vies, de la santé, des biens, de l'environnement...).

Pour construire et démontrer des performances de sécurité :

— on ne peut pas décider des conditions d'utilisation et d'environnement de l'entité ; il faut bien prendre en compte tout ce qui peut se présenter, mais on peut – on doit – pondérer en fonction de la vraisemblance de telle ou telle condition ;

— on ne peut pas toujours décider de l'usage qui sera fait de l'entité (en particulier, si l'entité est aux mains du public et non de professionnels), mais on peut – on doit – prendre en compte l'effet du mode d'emploi, qui, normalement, réduit, mais n'élimine pas les risques.

L'accomplissement de certaines fonctions, qu'on qualifiera alors généralement de fonctions de sécurité, peut être un moyen d'assurer la sécurité ; les exigences de fiabilité à l'égard de ces fonctions sont alors très sévères, tant en durée de bon fonctionnement exigée qu'en conditions dans lesquelles le bon fonctionnement doit être assuré.

Pour cette raison, dans un premier type de cas, la sécurité apparaît comme la fiabilité appliquée à des cas où l'accomplissement de la fonction est très important, c'est-à-dire que la panne est très grave et très rare.

Elle peut alors apparaître comme un cas particulier du calcul de fiabilité, le cas des valeurs extrêmes.

Dans un autre type de cas, la sécurité apparaît comme la maîtrise de tous les effets, produits, impacts de l'entité considérée qui ne sont pas souhaités et requis par le cahier des charges.

C'est en particulier dans ce dernier cas qu'apparaît une branche très développée de la sécurité qui est l'évaluation des conséquences d'un accident.

Il s'agit de développements particuliers de sciences diverses qui se rejoignent.

Par exemple, les calculs très complexes de modèles de déplacement et de dispersion de nuages toxiques ou radioactifs, ou bien les évaluations d'impacts sur la santé d'exposition des contaminations biologiques, chimiques, radioactives, ou encore les calculs de résistance d'ouvrages aux séismes, aux impacts, etc.

En tant que résultat dû au client, au public... la sécurité relève de ces deux approches qui peuvent interférer l'une avec l'autre, ce qui justifie la volonté de les traiter ensemble.

La première relève de la« théorie de la fiabilité », elle est intimement liée avec l'approche *F, M, D* ; la seconde relève d'approches de sécurité plus anciennes et toujours en progrès.

Issues de cultures différentes dans beaucoup de domaines industriels, ces approches gagnent désormais à être conduites ensemble.

Les définitions du « Petit Robert » nous confortent dans la convergence entre le sens usuel et celui que nous donnons à la sécurité :

— état d'esprit confiant et tranquille d'une personne qui se croit l'abri du danger ;

— situation, état tranquille qui résulte de l'absence réelle de danger(d'ordre matériel ou moral) ;

— organisation, conditions matérielles, économiques, politiques propres à créer un tel état, la situation obtenue ;

— sécurité sociale ;

— de sécurité, se dit de choses capables d'assurer la sécurité désintéressés.

Chapitre III

III. Taux de défaillance, MTBF, MTTF, MUT

III. Taux de défaillance, MTBF, MTTF, MUT

Les notions de fiabilité et de maintenabilité d'une entité étant définies (§ 2.3 et 2.4), on peut utiliser les mathématiques pour définir à partir des fonctions $R(t)$ et $M(t)$ de nouvelles grandeurs.

_ Le **taux de défaillance**, généralement noté $\lambda(t)$, est :

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

Il représente l'intensité de défaillance en fonction du temps.

C'est la probabilité conditionnelle, divisée par dt, de tomber en panne entre t et t + dt sachant qu'au temps t l'entité n'est pas défaillante.

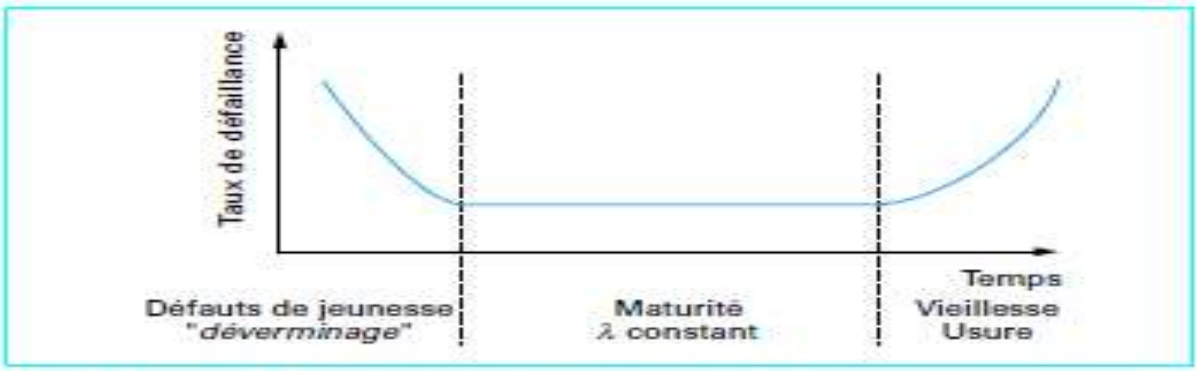


Figure 2 – Taux de défaillance d'une série de composants : courbe en baignoire

L'hypothèse est très souvent faite que ce taux de défaillance est constant (indépendant du temps). Alors la loi de fiabilité prend une forme facile à manipuler de :

$R(t) = \exp(-\lambda t)$

En fait, cette hypothèse très pratique est assez audacieuse, mais l'expérience a montré que, pour de nombreuses catégories de composants, il y avait une période assez longue entre la jeunesse et la vieilles se pendant laquelle cette hypothèse était une approximation tout à fait acceptable (encore faut-il vérifier qu'on exploitera effectivement cette seule période de la vie des composants si on a pris cette hypothèse pour les calculs prévisionnels).

On constate souvent que la courbe représentant le taux de défaillance d'une série de composants en fonction du temps à la forme dite « **courbe en baignoire** » (figure **2**) :

— la décroissance rapide de la fréquence des défaillances correspond bau « déverminage » et à l'élimination des défauts de jeunesse ;

— le fond de la baignoire correspond à la période de maturité où le taux de fiabilité des composants est le meilleur et, souvent, à peu près constant ;

— enfin, la remontée progressive de la fréquence des défaillances correspond à la vieillesse.

Si cette évolution est connue, on arrête généralement l'utilisation de ces composants avant que cette remontée du taux de défaillance soit significative. Si le retrait des composants n'est pas intervenu avant pour d'autres raisons, il intervient là en raison de la dégradation de la fiabilité.

Dans ce cas, la durée de vie des composants a été déterminée par leur fiabilité.

Contrairement à ce qui est souvent sous-entendu, la durée de vie d'un composant n'est pas nécessairement déterminée par la sortie de sa fiabilité des taux acceptables ; elle peut s'achever avant par l'arrivée sur le marché d'un concurrent préférable, par la disparition du besoin, par une exigence de performance qu'il ne peut satisfaire ,etc.

Ne pas prendre en considération la durée de vie réaliste du composant(avec toutes les raisons qui peuvent mettre fin à son utilisation),revient à concevoir et bâtir pour l'éternité, ce qui expose à retenir des exigences de sûreté de fonctionnement excessives.

_ Le taux de réparation, généralement noté $\mu(t)$, est :

$$\mu(t) = \frac{-\mathrm{d}M(t)/\mathrm{d}t}{M(t)}$$

Si on le suppose constant : $M(t) = \exp(-\mu t)$

_ Couramment, on utilise aussi la **moyenne des temps de bon fonctionnement** ou **MTBF**, mais ce paramètre très apprécié fait l'objet de confusions qui peuvent porter à conséquence.

À l'origine des confusions, il y a un jeu de mots : en anglo-américain, on utilise les deux sigles MTTF (*Mean Time To Failure*) et MTBF (*Mean Time Between Failures*).

Ce dernier sigle peut donc se transposer directement en français en MTBF (Moyenne des Temps de Bon Fonctionnement),mais pas avec la même signification.

Le **MTTF** est la moyenne des durées de fonctionnement de l'instant0 à la première défaillance.

Le **MTBF** est la moyenne des temps séparant deux défaillances consécutives.

Pour une entité réparable, connaissant une alternance de périodes de fonctionnement ininterrompu et de périodes de remise en état de fonctionnement, le MTBF est la moyenne de durées dont chacune est constituée d'une période de remise en état après défaillance suivie d'une période de fonctionnement ininterrompu.

On appelle MUT (*Mean Up Time*) la moyenne des temps de fonctionnement.

En général, un système satisfaisant connaît des périodes de panne beaucoup plus courtes que les périodes de bon fonctionnement ininterrompu ; de ce fait, le MTBF est à peine plus élevé que le MUT et la confusion entre les deux peu importante.

Parmi les erreurs d'interprétation les plus courantes touchant le MTBF, il y a celle qui consiste à croire que le MTBF est le temps pendant lequel on peut espérer être épargné par les défaillances.

Pour illustrer le danger de ce type d'interprétation, considérons le cas très usuel où l'hypothèse du taux de défaillance constant est retenue ;on a alors :

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

et la probabilité de ne pas avoir eu de défaillance après un temps égal au MTBF est :

R(MTBF) = exp (−1) ≈ 0,37

et, au bout de 2 MTBF, environ 0,15. Elle n'est encore que de 0,57après un demi-MTBF !

_ La figure **3** est une illustration des temps dont les moyennes servent de mesure de la sûreté de fonctionnement

_ **TTF** signifie *Time To Failure* : c'est le temps qui sépare l'instant zéro de la mise en service de la première défaillance.

Le MTTF est la moyenne sur un ensemble d'entités (par exemple de composants)considérés comme identiques.

_ **TTR** signifie *Time To Repair* : c'est le temps qui sépare, pour une entité réparable, la cessation de l'aptitude aux fonctions requises de sa reprise.

Le MTTR (*Mean Time To Repair*) est la moyenne sur un ensemble d'entités « identiques » et sur l'ensemble des cycles défaillance / réparation de la durée de vie considérée des TTR.

Il peut être utile de distinguer TTR et DT (*Down Time*) quand on veut séparer, à l'intérieur du délai qui sépare la défaillance de la reprise du service (délai global qu'on appelle alors DT), le délai dû à la réparation proprement dite, qu'on appelle alors TTR et qui ne dépend que de la conception de l'entité des délais dus à l'organisation de l'exploitation et de la maintenance).

Nous n'avons pas retenu ici cette distinction, mais elle peut être utile.

Il est surtout important de retenir que l'on ne peut se fier aveuglément aux mot set qu'il faut se faire préciser le sens dans lequel le partenaire l'utilise ,soit par une explicitation de la définition, soit par référence à une norme commune.

_ **UT** signifie *Up Time* : c'est le temps pendant lequel l'entité ne cesse d'être apte à remplir les fonctions requises dans les conditions données.

Le MUT est la moyenne sur un ensemble d'entités« identiques » et sur leurs durées de vie considérées des UT.

_ **TBF** signifie *Time Between Failures* : c'est le temps qui sépare deux défaillances consécutives.

Le MTBF est la moyenne sur un ensemble d'entités « identiques » et sur leurs durées de vie considérées des TBF.

Comme :

$$TBF = UT + TTR,$$

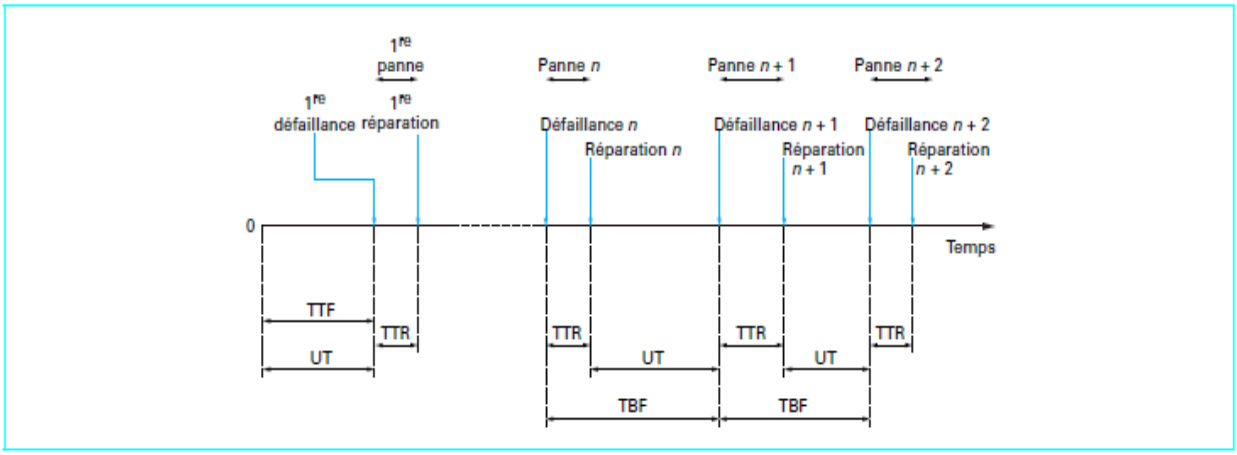


Figure 3 – Vie d'un système : évolution dans le temps

On a :

$$MTBF = MUT + MTTR$$

En général, en France, on utilise les sigles d'origine américaine MTBF, MTTF, MTTR et MUT, avec le risque de mal se comprendre évoqué au début du paragraphe ; on peut proposer

Les expressions françaises suivantes pour utiliser exactement les mêmes notions en levant les ambiguïtés :

TTR temps de réparation,

TTF temps avant défaillance,

UT temps de bon fonctionnement,

TBF temps entre défaillances.

Chapitre IV

IV. Données de fiabilité (ou de maintenabilité)

IV. Données de fiabilité (ou de maintenabilité)

IV.1 Généralités

Comme nous l'avons souligné (§ 1.2), une démarche de sûreté de fonctionnement exploite des connaissances.

Sans connaissances, il n'y a pas d'analyse de risques possible.

Ces connaissances sont de nature **qualitative** (fonctionnements des systèmes, sensibilités aux agressions, enchaînements causes – conséquences...) **et** de nature **quantitative** ou chiffrée : ce sont, par exemple, des taux de défaillance de composants, des fréquences de telles ou telles conditions de température, de crue, etc., des probabilités d'événements ,des probabilités conditionnelles, des coûts d'événements, des étendues d'atteinte à l'environnement, etc.

Parmi toutes ces connaissances utiles, certaines s'expriment par des **probabilités**, soit que l'on ait affaire à des phénomènes réellement aléatoires, soit que l'on ait affaire à un ensemble complexe de phénomènes sans doute déterministes mais mal connus et que la loi des grands nombres permet d'approcher de façon pertinente, pour le niveau des décisions en jeu, sous forme d'une loi de probabilité.

Ces données probabilistes occupent le devant de l'affiche à tel point que l'on peut penser que la sûreté de fonctionnement n'est faite que de calcul de probabilités.

Cette impression est d'ailleurs entretenue par beaucoup de formations à la SdF qui commencent par des « rappels de probabilité ».

En fait, cette partie de la Sdf est la plus visible parce que la plus technique, celle qui justifie le plus une expertise de spécialiste et celle qui, par sa technicité et l'importance des mathématiques, donne la plus forte impression de certitude, d'objectivité... Or, si la rigueur des calculs est inattaquable, la valeur des conclusions dépend totalement de la validité de la représentation de la réalité par les objets mathématiques utilisés (lois de probabilité, liens logiques, valeurs des paramètres, etc.) et de l'exactitude des données utilisées.

Il ne faut surtout pas sous-estimer l'importance de toutes les données, en particulier qualitatives, et garder toujours présente à l'esprit la question de la validité des représentations utilisées et de leurs limites.

Si ces bases sont solides, l'édifice de calculs bâti dessus ne posera pas de problèmes.

_Où trouve-t-on les données ? Les modèles mis au point et reconnus par la recherche scientifique depuis des siècles et jusqu'à nos jours, les expériences cumulées par les uns et les autres constituent les réserves d'informations à disposition des « fiabilistes ».

Deux démarches spécifiques à la sûreté de fonctionnement jouent un rôle essentiel : les bases de données et le retour d'expérience.

Bien souvent, manquant de données nécessaires, on organise de essais et des tests pour produire de la connaissance, de l'expérience, donc des données.

IV.2 Bases de données

La possession ou l'accès aux données de fiabilité ou de maintenabilité sont une ressource extrêmement précieuse pour évaluer des risques.

Ces données peuvent être **propres au système** dont on a la charge et il faut constituer soi-même sa base de données. L'emprunt à d'autres bases de données qu'on sait adapter à son cas, les essais préalables, le retour d'expérience sont les sources principales.

Ces données peuvent, au moins en partie, être **communes à d'autres systèmes** et l'effort de constitution des bases pourrait être partagé.

Les composants de base en électronique d'abord, puis dans d'autres domaines, étant communs à de nombreuses industries, on gratuits ou payants, des données comme des tableaux de taux de défaillance de composants.

Cette mutualisation peut être le fait d'une action publique ; divers organismes publics comme le CNET en France ont mis ou mettent gratuitement à disposition des bases de données de fiabilité.

Cela peut être des activités de service public accessibles à titre on éreux ou des activités commerciales.

Elle est aussi assez souvent le fait de groupements d'entreprises ou de branches professionnelles qui constituent des bases de données privées accessibles seulement aux membres qui en assurent l'alimentation et le financement.

Certains fournisseurs accompagnent leurs fournitures de données– des lois de fiabilité, des taux de défaillance – et, dans certains cas, s'engagent sur celles-ci.

Bien des industriels constituent leurs propres bases de données et les enrichissent par des échanges avec d'autres entreprises.

IV.3 Retour d'expérience

Le principe du retour d'expérience est d'améliorer sa connaissance du système par l'observation, le recueil, l'analyse, le traitement des informations relatives au fonctionnement réel du système, à son environnement, à son impact sur son environnement [7].

Améliorer sa connaissance, ce peut être la compléter, l'enrichir, la rectifier, mais c'est certainement réduire les incertitudes et augmenter la confiance sur la connaissance que l'on a du système.

On considère généralement que le retour d'expérience consiste à remplir des bases de données avec les caractéristiques des événements redoutés qui se produisent, au fur et à mesure de leurs survenues. Une démarche de retour d'expérience est bien plus que cela et pour être la plus utile et la moins coûteuse, ne consiste pas forcément recueillir systématiquement ces descriptions d'événements [6].
En fait, une **démarche de retour d'expérience**, décidée non pas par principe (parce que ça se fait) mais pour en tirer profit, est orientée vers la réduction des incertitudes influentes dans l'analyse des risques.
Le retour d'expérience n'est pas une démarche ponctuelle, opportuniste.
C'est à l'occasion de décisions dans lesquelles des analyses de risques sont prises en compte qu'il joue un rôle.
Nous avons vu (4.1) que l'analyse de risques s'appuyait sur la connaissance du
Système , de son environnement, de son utilisation, etc.
Il y a toujours de grandes incertitudes dans cette connaissance (pas seulement dans les données quantitatives, mais aussi dans la connaissance des fonctionnements du système).
Le retour d'expérience à pour but de réduire ces incertitudes, en corrigeant, éventuellement, des erreurs.
Un retour d'expérience peut être optimal si l'on a pu anticiper les connaissances qui entreront un jour ou l'autre dans des analyses de risque nécessaires à des décisions, si l'on a pu prévoir le niveau de précision juste nécessaire pour optimiser la décision.
Alors, on peut organiser et dimensionner un retour d'expérience pour satisfaire précisément ces besoins... ni trop, ni trop peu.
Un retour d'expérience, qui recueille des informations (permettant de connaître la réalité des scénarios possibles et la valeur réelle des paramètres de fiabilité ou de maintenabilité) et qui les traite, signale donc les écarts entre la réalité et les hypothèses des études de risque.
De ce fait, il peut être à l'origine de **décisions** :
— mesures conservatoires ;
— révisions d'études de risques et mesures de réduction de risques complémentaires qui en découlent ;
— organisation d'investigations d'un suivi plus précis, plus fin, d'un certain point ;
— tests ou essais pour apprécier la réalité et la représentativité de ces écarts.
Sur un système jeune, il est difficile de dire si quelques défaillances vite arrivées sont significatives d'un taux de défaillance nettement plus élevé que prévu ou du hasard.
Et s'il s'agit d'un taux de défaillance plus élevé que prévu, est-ce parce qu'on est encore

dans une phase de jeunesse des composants ou est-ce parce que leur taux de défaillance de maturité est plus élevé que prévu ?

De très nombreux retours d'expérience consistent, sans se oser autant de questions, à **recueillir les événements redoutés** et à **les compter** (ou à compter des événements considérés comme causes des incidents recueillis).

Ce n'est pas un hasard, car cela correspond à une situation courante ; on craint de n'avoir pas imaginé tous les scénarios possibles conduisant aux accidents et on manque de précision ou de confiance sur les fréquences des événements initiateurs.

Alors, il est normal, pour affiner ses choix de conception et d'exploitation et veiller à rester proche d'un optimum quand les conditions extérieures changent, de rechercher les scénarios non prévus qui se réaliseraient (d'où le recueil de tous les accidents, incidents... et l'identification pour chacun du scénario qui s'est réalisé), et d'évaluer la fréquence réelle des événements initiateurs
(Ceux dont la fréquence a priori a servi à évaluer les risques), d'où le décompte du nombre d'événements qui, rapporté au temps, donne cette fréquence réalisée.

Un retour d'expérience peut être **organisé autour de deux idées**.

_ Approche à dominante qualitative : recueillir et analyser chacune des occurrences des incidents ou accidents « significatifs ».

Dans ce contexte, il s'agit des événements dont la gravité est assez élevée pour que la fréquence acceptable ne soit pas infinie [événements inacceptables ou acceptables en dessous d'une certaine fréquence (cf. figure **1**)].

Le retour d'expérience a alors pour **fonction première** de s'assurer que ces incidents se sont réalisés selon les scénarios prévus ou alors de repérer un scénario – possible puisque réalisé – qui n'était pas imaginé ou que l'on croyait avoir rendu impossible.

De telles découvertes conduisent à réviser les analyses de sûreté de fonctionnement,
voire à des mesures conservatoires urgentes si la gravité de l'événement concerné est élevée.

Secondairement, ce recensement des événements permet de comparer leur nombre de réalisations à la fréquence acceptée.

Approche à dominante quantitative: recueillir et comptabiliser les événements ou les conditions dont la fréquence prévisionnelle a été utilisée dans les évaluations de sûreté de fonctionnement.

L'accumulation de ces statistiques fournit des données de fiabilité issues directement de la réalité ; leur précision croît avec le temps et le nombre d'observations et elles permettent de réviser les données utilisées dans les évaluations.

À l'aide de techniques statistiques, éventuellement assez sophistiquées, on peut tirer le meilleur parti de ces données de retour d'expérience (en tenant compte de leurs limites), des avis d'experts et des données a priori issues de bases ou de modèles théoriques(toujours un peu simplificateurs), afin d'avoir le meilleur couple précision/confiance sur les données de fiabilité qui servent aux évaluations.

On remarque l'importance de se fonder sur une démarche d'évaluation a priori pour cibler les données à préciser plutôt que recueillir de l'information tous azimuts et brasser d'énormes quantités de données avec des résultats souvent décevants.

Chapitre V

5. Démarches et méthodes fondamentales d'une approche Sdf

5. Démarches et méthodes fondamentales d'une approche Sdf

5.1 Présentation des caractéristiques

Dans le tableau **1**, nous avons essayé de caractériser la démarche ou méthode citée : inductive ou déductive, quantitative ou qualitative et sa fonction. Attention, cette dernière peut être très réductrice ! **Démarches ou méthodes**, la distinction est discutable.

Ce que nous avons qualifié de méthodes est étroitement encadré par un raisonnement et une mise en forme alors que ce que nous avons qualifié de démarches est caractérisé par un état d'esprit, une démarche intellectuelle mais peut prendre des formes extrêmement variées, tant dans la mise en œuvre que dans la présentation des résultats.

Les méthodes qui décrivent des liens causes/conséquences partent des causes pour en déduire les conséquences, on les dit **inductives**, ou partent des conséquences pour remonter aux causes, on les dit **déductives**.

L'un est exclusif de l'autre, mais une approche par une méthode inductive est judicieusement complétée par une approche déductive et réciproquement.

Il n'y a pas de recherche de quantification sans analyse qualitative.

Par contre, il peut y avoir analyse qualitative sans quantification.

Nous avons donc qualifié de **quantitatives** les méthodes qui offraient une possibilité importante de quantification (de fréquence)et de **qualitatives** les méthodes qui l'excluaient ou dans lesquelles cet aspect est marginal.

L'objectif de la présentation des méthodes et démarches est de les caractériser rapidement et de les situer les unes par rapport aux autres.

Leur mise en œuvre relève d'articles spécialisés, que le lecteur trouvera dans le CD-Rom Sécurité/Prévention des risques.

5.2 Analyse préliminaire de risques (APR)

Cette **démarche** a pour but de produire une liste d'événements redoutés qui doivent être étudiés.

Elle cherche, d'une part, à faire un tour aussi complet que possible des événements redoutés (accidents ou défaillances) et, d'autre part, à écarter rapidement ceux qui ne pourraient conduire à des conséquences assez importantes pour justifier les études.

C'est un concept très lâche.

On a l'habitude de la qualifier de « ***méthode de Sdf*** ».

Dans le sens où méthode évoque des règles, un ordre, une procédure normée reproductible, l'APR en est très éloignée.

Elle prend des formes très différentes selon les pratiques : cela va d'un court tableau très

synthétique, bâti en une heure ou deux à la lumière de listes types, à une étude très complète et assez détaillée des risques qui concernent un système, en passant par tous les intermédiaires imaginables. Elle est un peu à elle seule un **résumé d'une démarche de maîtrise des risques** par la Sdf :

— identification des événements redoutés, mais sans entrer dans les détails ;

— évaluation et acceptation des risques : il s'agit sommairement de retirer de la liste les événements qui sont, a priori, sans doute clairement en dessous du seuil à partir duquel ils méritent attention, Évaluation aussi précise que possible et arbitrage ;

— maîtrise : mesures propres à réduire et contenir les risques aux niveaux acceptables.

Tableau 1 – Principales démarches et méthodes de base de SdF

Démarches/ Méthodes	Inductive/ déductive	Quantitative/ qualitative	Phrase-clef
Retour d'expérience	Déductive	Quantitative	Alimenter sa connaissance du système à la réalité
Analyse préliminaire de risques (APR)	Inductive	Qualitative	Repérer *a priori* les risques à étudier
Analyse des modes de défaillance et de leurs effets (AMDE)	Inductive	Qualitative	Recenser les conséquences des défaillances
Analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC)	Inductive	Quantitative	Évaluer les conséquences des défaillances
Arbre de causes	Déductive	Qualitative	Organiser les éléments ayant contribué à un accident
Arbre d'événement	Inductive	Quantitative	Évaluer les conséquences possibles d'un événement
Arbre de défaillances	Déductive	Quantitative	Évaluer les scénarios d'un accident potentiel
Graphes d'état	Inductive	Quantitative	Évaluer les états possibles d'un système réparable

Toute APR a pour **objectifs** :

— l'identification des événements redoutés (souvent limités à ce qui concerne la sécurité, généralement dans toutes les phases de vie du système) ;
— une évaluation permettant une hiérarchisation de ces risques ;
— l'identification des dispositions de réduction de risques qu'il faudra prévoir (donc spécifier, évaluer en termes de Sdf en particulier).

Elle est particulièrement importante dans un projet de système complexe réunissant plusieurs partenaires ayant un rôle significatif dans la sécurité.

Elle doit permettre, grâce à la vision globale des risques qu'elle offre, une vision commune à tous ces partenaires des risques, des besoins de réduction de risques, des rôles et responsabilités de chacun.

Cette démarche APR, ou APD (analyse préliminaire de danger) dans certains domaines avec quelques différences, est généralement une première étape indispensable quand des questions de sécurité sont posées.

Elle l'est beaucoup moins s'il n'est question que de *F*, *M*, *D*. Quand elle est réalisée dès le début, elle sert aussi de référence tout au long du projet.

La clef d'une démarche APR est la liste (dans la tête des experts ou dans des documents *ad hoc*) des éléments qui peuvent se réunir pour provoquer un accident : entités dangereuses et situations dangereuses.

ANALYSE DES MODES DE DÉFAILLANCE, DE LEURS EFFETS ET DE LEUR CRITICITÉ (AMDEC)

Origine : AMDEC : Produit/Projet Analyste : Date : 17/06/95: Folio
Pièce : NUMÉRO : AGRAFE

FONCTIONS (ET/OU) PROCESSUS	DÉFAILLANCE				GRAVITÉ	FRÉQUENCE	DÉTECTION	ACTION	Responsable	Délai
	MODE	CAUSE	EFFET	DÉTECTION						
Ôter une agrafe d'une liasse de papier	Impossible d'accrocher l'agrafe avec les mors	Forme de l'extrémité des mors trop arrondie P1 : 10 % P21 : 100 %	Impossible d'arracher l'agrafe	Essais de formes	9	9	2			
	Impossible d'exercer la traction sur l'agrafe	Frottement entre les deux mâchoires P1 : 1 % P21 : 0,1 %			6	3	10	Utilisation de deux mâchoires chromées	D. Dupont	20/06/95
		Coincement de l'agrafe entre les deux mâchoires P1 : 1/3 P21 : 1			6	10	10			

Figure 4 – Extrait d'un tableau d'AMDEC

Une APR se fonde sur l'identification des situations que peut connaître le système pour isoler les situations dangereuses.

La connaissance des éléments qui constituent le système est la base pour repérer les composants potentiellement dangereux, les sous-systèmes de sécurité et leurs fragilités.

L'étude du Groupe de Travail et de Réflexion no 55 de l'I Sdf sur l'APR [4] confirme que la méthode conduite d'une APR n'est pas et ne doit pas être normalisée, mais elle présente en annexe plusieurs exemples ou témoignages qui confirment la philosophie commune et la variabilité des formes qu'elle peut prendre (et ce n'est encore que dans un domaine : le ferroviaire !).

5.3 Analyse des modes de défaillance, de leurs effets et de leurs criticités (AMDEC)

C'est la méthode la plus citée au point d'être parfois confondue avec la sûreté de fonctionnement, sans doute aussi la plus utilisée jusqu'à l'abus.

Le principe est le suivant :

— décomposer le système en éléments bien connus ; le niveau de détail de la décomposition se détermine sur ce critère : le niveau auquel on sait associer des modes de défaillance et des fréquences si possible ;

— associer à chaque élément ses modes de défaillance ; chaque mode de défaillance est une façon dont il se comporte à part son comportement prescrit ;
— identifier les effets sur le système de chaque mode de défaillance de chaque élément ;
— éventuellement (c'est cette étape qui distingue l'AMDEC de l'AMDE, Analyse des modes de défaillance et de leurs effets), associera chacun des modes de défaillance de chaque élément sa criticité, en fonction des effets qu'il produit.
Bien entendu, cette analyse cause/conséquence n'a d'intérêt que si l'on en tire des conclusions. Aussi, les diverses normes officielles, ou de fait, sur l'AMDEC comprennent-elles des suites relatives à l'exploitation de cette analyse qui sont un peu différentes selon le cadre dans lequel la méthode est utilisée (cf. plaquette AMDEC, ISF[5]).

5.4 Arbres de causes, d'événement ,de défaillances

Les représentations de liens logiques causes/conséquences partant d'un événement ont une forme arborescente. Nous évoquons ici trois formes très usitées.
Un arbre de cause s'explicite la façon dont des combinaisons d'événements et de conditions ont conduit à la réalisation d'un accident.
C'est une représentation logique de l'analyse des causes d'un accident (il n'utilise que le connecteur logique ET).
À une extrémité, on trouve l'accident ou l'incident analysé et aux extrémités des ramifications, les événements, conditions ou circonstances qui se sont rencontrées pour qu'il se produise.
L'appellation « *arbre de causes* », qui aurait aussi bien pu être retenue pour désigner les arbres de défaillances a été retenue pour désigner la méthode de représentation de l'analyse *a posteriori* d'un accident.
Elle a été très bien promue dans le domaine de la sécurité au travail et largement diffusée par l'INRS (Institut National de Recherche et de Sécurité) dans ce cadre.
La construction d'un arbre de causes (figure **5**) consiste à partir de l'événement final et à remonter, étape par étape, en se demandant à chaque fois, quelle est la combinaison d'événements, d'actions, de décisions, de conditions qui a provoqué l'événement immédiatement supérieur.
Il importe, pour profiter de cette méthode, de ne jamais se censurer en ne retenant que ce qui serait une cause au sens strict, mais, au contraire, de noter tout ce qui a joué un rôle.
Un arbre d'événement part d'un événement (origine), et on s'interroge sur les conséquences qu'il peut avoir.
Quand on se pose cette question, on suit un chemin jalonné de « si telle condition est remplie, alors..., dans le cas contraire... ».

On représente ce raisonnement sous forme d'un schéma qui se lit usuellement de gauche (une entrée unique : l'événement dont on cherche les conséquences) vers la droite (les événements ultimes dont il peut être une cause) en progressant de bifurcation en bifurcation, le nombre de branches croissant au fur et à mesure que l'on progresse vers les conséquences en explorant à chaque fois les deux branches des alternatives qui s'ouvrent.

On en retire donc la liste des conséquences possibles d'un événement(figure **6**), la probabilité de chacune si on connaît la probabilité qui affecte chaque alternative ; on peut évaluer l'effet de certaines mesures en regardant comment l'arbre s'en trouve modifié.

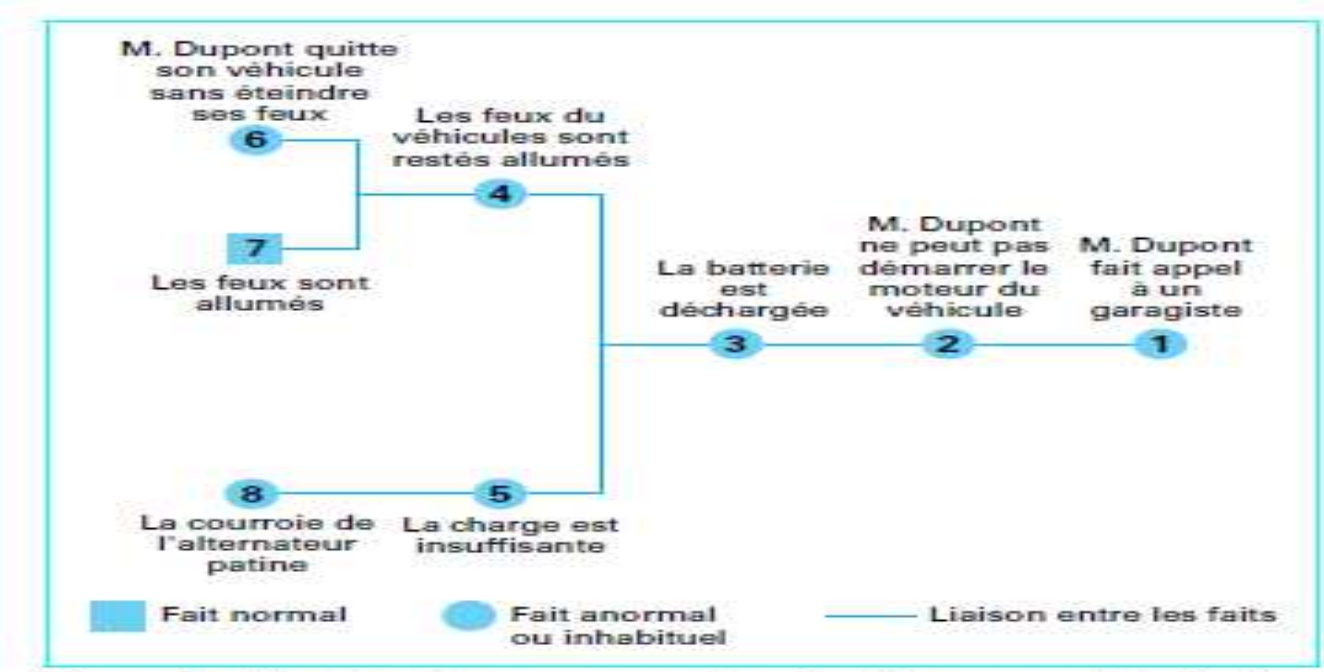


Figure 5 – Un arbre de causes pour le scénario « panne de batterie »

Les diagrammes cause-conséquence (non illustrés ici) représentent sous une autre forme la même chose.

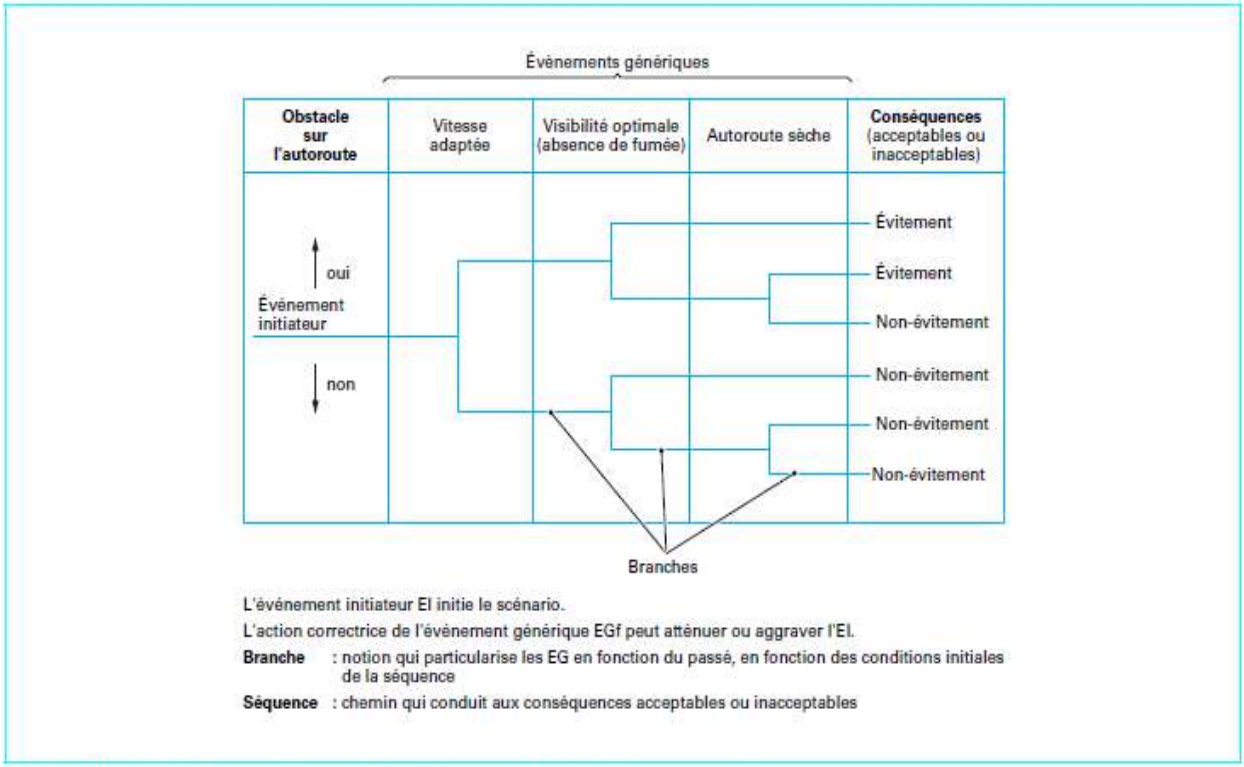


Figure 6 – Un arbre d'événement pour le scénario « évitement d'un obstacle sur l'autoroute »

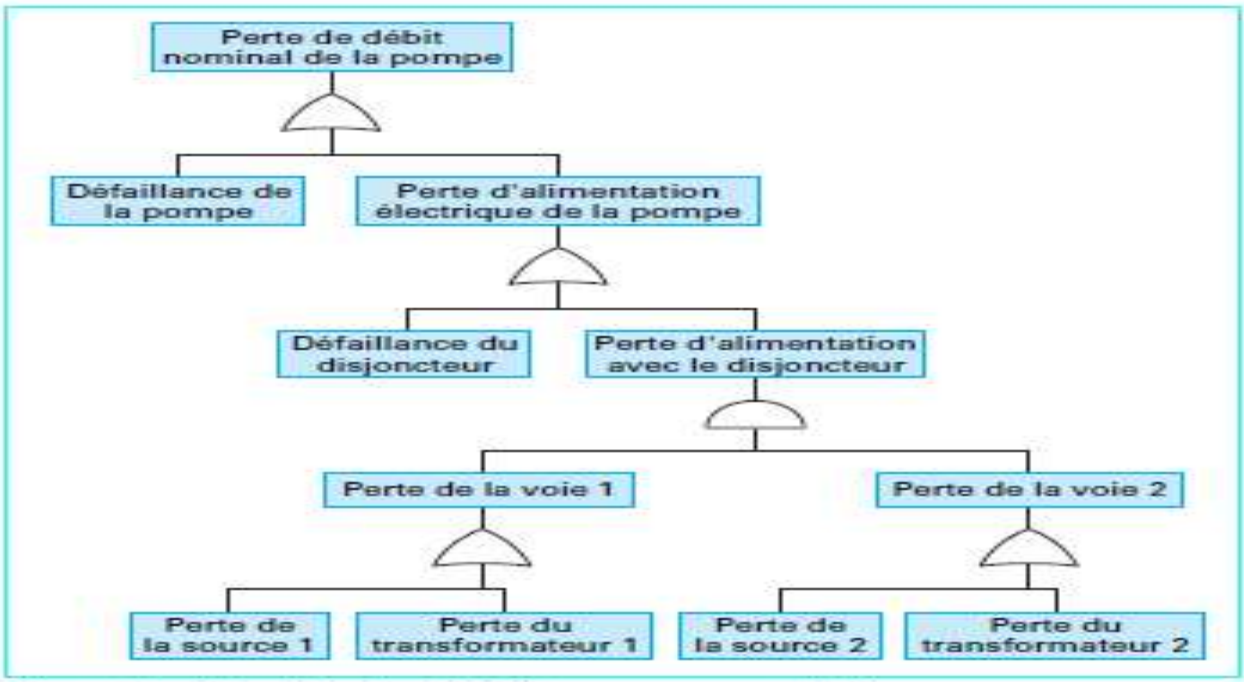


Figure 7 – Un arbre de défaillances : exemple d'une pompe électrique

Un arbre de défaillances modélise l'ensemble des combinaisons d'événements et de conditions qui peuvent aboutir à l'événement sommet (il utilise tous les connecteurs logiques « ET », « OU »inclusif et exclusif et leurs combinaisons).

Un arbre de causes est un scénario inclus dans l'arbre de défaillances.

L'arbre de défaillances, si l'on a pu tout imaginer, inclut tous les arbres de causes possibles.

Comme les liens sont des fonctions logiques, la probabilité de l'événement« sommet » se déduit par algèbre booléenne des probabilités des événements « feuilles ».

_ La construction d'un arbre de défaillances (figure **7**) consiste à sélectionner un événement dont on veut représenter les scénarios de survenues.

On se pose la question « quels événements ou combinaisons d'événements et de conditions pourraient produire cet événement ? ».

On représente donc, avec des connecteurs logiques(OU, ET, éventuellement des OU exclusif, *p*/*n* – par exemple 2/3 ou3/4... –), les réponses trouvées.

Puis on réitère : on se demande comment peuvent se produire ces événements qui, combinés de certaines façons, peuvent produire l'événement qui nous intéresse et ainsi de suite.

On arrête de décomposer chaque fois qu'on arrive à des événements sous des conditions dont on connaît bien le cas ou la fréquence d'apparition.

_ Cette représentation permet de **déduire la probabilité de l'événement redouté** « sommet » (le point de départ de l'étude) des probabilités des événements « feuilles » sur lesquels la décomposition s'est arrêtée.

Elle permet aussi d'établir la liste des combinaisons d'événements et de conditions suffisantes pour provoquer l'événement étudié.

Une telle combinaison est appelée une « coupe » et on s'intéresse en priorité aux coupes minimales: la suppression d'un seul élément d'une coupe minimale (une réparation ou le retrait d'une condition) le rend insuffisant pour provoquer l'événement« sommet ».

Une coupe minimale est un ensemble nécessaire et suffisant d'événements et de conditions pour provoquer l'événement sommet.

On associe à chacune de ces combinaisons (coupes minimales de l'arbre) la part qu'elle représente dans la probabilité totale de survenue de l'événement sommet, ce qui permet de hiérarchiser les tentatives de prévention de l'événement étudié.

On peut chercher à **vérifier** si une **règle** comme « une seule défaillance ne doit pas pouvoir provoquer tel accident » est respectée : on bâtit l'arbre de cet accident et on cherche les « coupes minimales d'ordre 1 », c'est-à-dire les événements qui suffisent à eux seuls à provoquer l'accident.

S'il y a parmi eux des défaillances, la règle n'est pas respectée » et on sait où !

Si la règle est moins simple comme « un accident ne peut résulter que d'au moins trois défaillances dans les conditions normales et d'au moins deux dans des conditions exceptionnelles », la même démarche permet de s'assurer que la règle est respectée ou d'identifier ce qu'il faut faire pour la respecter.

De même, un **arbre** de défaillances permet d'**évaluer l'effet d'une mesure** à prendre, d'une modification du système sur la probabilité de survenue d'un événement. Il permet de recenser les différents scénarios de survenue de l'événement sur lesquels la mesure envisagée aurait un effet, de les évaluer et des additionner.

Toutefois, si l'arbre de défaillances est une méthode remarquable de représentation synthétique des scénarios conduisant à un événement redouté, il a ses **limites**.

Il est difficile de représenter des aspects temporels un tant soit peu complexes. Si les mêmes événements intermédiaires ou « feuilles » apparaissent à plusieurs endroits, les calculs simples et automatiques sont faux ; il en va de même si les événements « feuilles » ne sont pas indépendants entre eux.

Le principe des coupes minimales ne fonctionne pas si un événement(comme une panne) entre dans certaines combinaisons pour provoquer l'événement « sommet », mais entre dans d'autres pour empêcher cette survenue (des pannes qui dans certaines circonstances réparent ou compensent d'autres pannes.).

5.5 Graphes d'états. Réseaux de Petrie

Moins utilisés mais encore assez courants sont les **graphes d'Etat**.

Chaque état du système est caractérisé par le fonctionnement ou non-fonctionnement des éléments P1 et P2.

Ces états En sont reliés entre eux par des arcs qui représentent les transitions possibles (figure **8**) : les défaillances caractérisées par le taux de défaillance λ et les réparations caractérisées par le taux de réparationμ.

Les algorithmes de calcul applicables à de tels modèles permettent d'évaluer la proportion du temps passé dans chacun des états en fonction des taux de défaillance et des taux de réparation.

On peut construire de tels graphes pour évaluer la fiabilité (donc la probabilité de ne pas être tombé en panne de l'instant 0 à l'instant) en inhibant les réparations ou la disponibilité (en prenant en compte défaillances et réparations).

C'est surtout dans ce deuxième cas que cette méthode révèle tous ses avantages.

Les **réseaux de Pétri** sont des outils très puissants de modélisation et de calcul.

Souvent cités parmi les outils de la sûreté de fonctionnement, ils ne sont utilisés que par de rares équipes à la pointe de ces techniques [1].

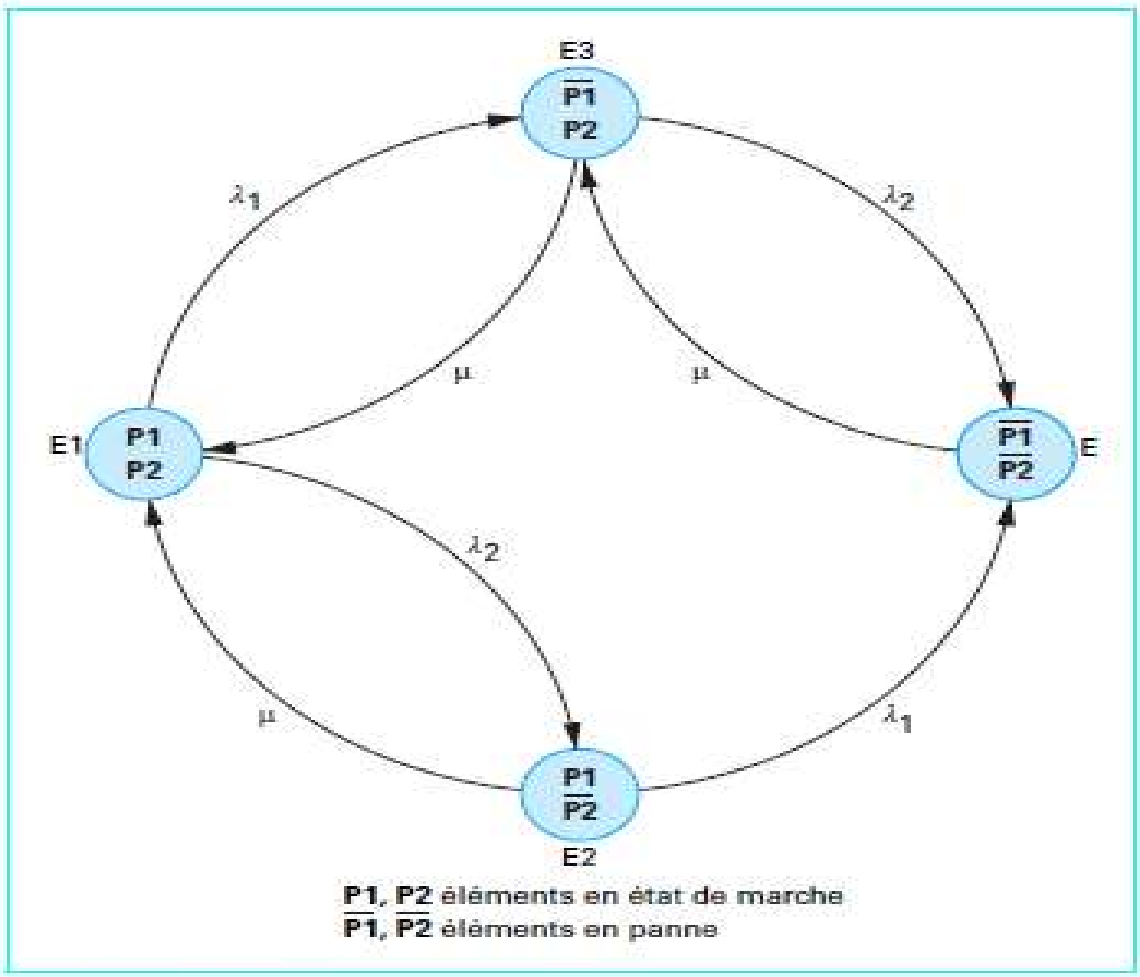


Figure 8 – Exemple de graphe d'état

5.6 Complémentarités entre ces méthodes

Il n'y a pas de règle qui fabrique la méthode universellement idéale en assemblant ces méthodes, mais leurs caractéristiques majeures leur assignent des rôles privilégiés.

L'**APR** est une démarche introductive qui permet de mieux focaliser ses efforts d'analyse de risque. Elle est précieuse en sécurité quand la préoccupation d'être exhaustif dans l'identification des risques est forte et difficile à satisfaire.

L'**AMDEC** est la démarche qui permet de réunir et d'exploiter des connaissances disponibles sur les défaillances des éléments composant le système étudié.

Elle a la réputation d'être exhaustive, ce qui est justifié si la connaissance des modes de défaillance au niveau où l'analyse est conduite est elle-même exhaustive et si la prise en compte des modes de défaillance suffit à atteindre les objectifs de l'étude.

L'**arbre de causes** est la méthode la plus propre à réunir l'ensemble des éléments explicatifs d'un accident (sans se limiter à ce qui peut être qualifié de causes).

L'**arbre d'événement** est adapté pour traiter la question « que peut-il arriver si... ? ».

L'**arbre de défaillances** est une représentation synthétique des scénarios d'accidents Contrairement à l'AMDEC, il rend bien compte des combinaisons de pannes ou d'événements. Comme l'AMDEC il ne rend pas compte des aspects temporels.

Il ne peut être construit que si on sait répondre aux questions : « qu'est ce qui peut conduire à... ? ».

Les **graphes d'états** sont particulièrement adaptés à l'évaluation de la disponibilité d'un système réparable ; les méthodes précédentes prenant difficilement en compte les réparations, sont plus adaptées à l'évaluation de la fiabilité (ou de la maintenabilité) ou à une approche sécurité.

Chapitre VI

6. Fiabilités électronique, mécanique, logicielle, humaine

6. Fiabilités électronique, mécanique, logicielle, humaine

Les différentes sciences sollicitées par la Sdf apportent des modèles très différents.

Le très grand nombre de **composants électroniques**« identiques » mis sur le marché (et le nombre élevé de défaillances)a permis de représenter leur fiabilité par une excellente approximation probabiliste grâce à la « loi des grands nombres ».

Il faut être conscient que cette approche probabiliste est pertinente en raison de cette « loi des grands nombres » et non parce qu'elle traduirait les lois de la physique.

C'est la même raison qui la fait utiliser à propos d'autres types de composants ; la pertinence de la loi des grands nombres est alors à réexaminer. Il n'est que trop courant d'ignorer cette base et donc de s'appuyer plus ou moins inconsciemment sur la loi des grands nombres à tort.

De même l'approximation si pratique du taux de défaillance constant est elle assez juste pour nombre de composants électroniques pendant la maturité de leur vie, mais c'est une hypothèse qui est souvent adoptée par défaut alors qu'elle est indéfendable.

En **mécanique**, les phénomènes d'usure sont souvent prépondérants, donc les taux de défaillance, quand ils sont un sens, ne sont guère constants.

La mécanique déterministe consiste à évaluer si la soustraction[résistance-contrainte] est positive.

La mécanique probabiliste consiste à évaluer la probabilité que la résistance soit supérieure à la contrainte, l'une et l'autre pouvant être représentées par des lois de probabilité, pas toujours indépendantes.

La grande majorité des systèmes mécaniques résolvent le problème par un sur dimensionnement: des « coefficients de sécurité », parfois fixés par les règlements, normes ou règles de l'art, imposent un dimensionnement propre à résister au pire cas ou, quand celui-ci est potentiellement infini, à une contrainte dont le dépassement est statistiquement peu probable (crues, vents, tremblements de terre décennaux, séculaires ou millénaires, etc.).

Toutefois, dans certains domaines (le spatial étant le cas extrême), il est essentiel de réduire la masse ou la quantité de matière au plus strict nécessaire et ces méthodes sophistiquées permettent d'associer le risque de rupture pris au dimensionnement choisi et de rechercher le plus juste équilibre.

Le comportement d'un **logiciel** est totalement déterministe, mais pas nécessairement prévisible.

Un système programmé produit des événements redoutés du fait des défaillances de ses composants physiques, d'effets d'agressions de l'environnement(rayonnement cosmique, perturbation électromagnétique, voire perturbations de l'alimentation ou interventions humaines

intempestives...),de l'exécution correcte des logiciels qui, dans certaines configurations, avec certaines données, produit un résultat non souhaité.

Les méthodes de conception de logiciels critique sont pour but de réduire les incertitudes sur de tels cas, d'une part, au niveau de la conception (validations des spécifications, etc.), d'autre part, au niveau de la réalisation (cf. cycle en « V », etc.).

Les méthodes de tests de systèmes programmé sont aussi pour objet de réduire les incertitudes (ils portent sur le couple matériel/logiciel) ; toute la difficulté est de savoir jusqu'à quel point un nombre forcément limité de configurations (matérielles, logicielles, données) est représentatif de toutes les combinaisons (combinatoire explosive) qui pourraient se présenter.

À l'inverse, le comportement d'un **homme** ou d'une **équipe** dépend d'une quantité d'influences et la même situation ne peut passe répéter (ne serait-ce que parce que l'expérience de la première fois différencie la seconde fois de la première).

Il est bien plus pertinent de parler de la fiabilité du **couplage homme-tâche** que de la fiabilité humaine.

Dans le cas de tâches répétitives exécutées dans des conditions identiques un grand nombre de fois, on peut caractériser la fiabilité humaine par le taux de succès de la tâche.

Il existe alors plusieurs modèles (simples comme TESEO ou plus complexes) et tables (dont les célèbres tables de Swain) qui donnent des valeurs prévisionnelles de ces taux de réussite en fonction de caractéristiques simples de l'opérateur et de la tâche [3].

Toutefois, dans les systèmes modernes, ces tâches sont de plus en plus souvent confiées à des automates et les tâches qui reviennent à l'homme sont des tâches complexes faisant appel à la richesse de ses sens, à ses capacités de synthèse et de diagnostic de situations complexes avec des informations incomplètes, voirie certaines, et à ses capacités de décision.

Dans ces cas-là, un modèle donnant une probabilité de succès ou d'échec ne peut représenter une réalité si complexe.

Les analyses poussées des accidents survenus dans les systèmes complexes (et « super sécurisés » [3] comme l'accident de centrale nucléaire de Three Miles Island ou celui de Tchernobyl, l'accident de plateforme de Piper Alpha, l'accident de l'aéroport de Ténériffe ou l'accident de chemin de fer de la gare de Lyon, etc. mettent en évidence des conditions favorables aux « erreurs » et des cheminements typiques des accidents (par exemple : comment une première erreur d'interprétation bénigne au stade où elle se produit et très compréhensible se transforme (on parle de biais de confirmation ,d'erreur diabolique...) : l'opérateur se construit une interprétation de plus en plus

éloignée de la réalité et de plus en plus accentogène pour faire cadrer avec sa première interprétation –erronée – les informations qui la contredisent).

Par ailleurs, les sciences de l'homme et des organisations, psychologie, sociologie, physiologie et biologie, les sciences de la décision progressent dans la connaissance du comportement des hommes et des équipes en particulier en situations de travail.

Ces connaissances sont peu à peu intégrées dans des pratiques et des approches d'études, de conceptions et/ou cliniques dont les plus connues en entreprise sont l'ergonomie (qui ne se réduit pas aux règles de l'art en matière de conception des postures, de l'éclairement ou du bruit et des interfaces homme-machine des postes de travail) et la médecine du travail.

Références bibliographiques

[1] LEROY (A.) et SIGNORET (J.-P.). – *Le risque technologique*, PUF Que sais-je ? no 2 669, 1992.

[2] VILLEMEUR (A.). – *Sûreté de fonctionnement des systèmes industriels*. Éd. Eyrolles, Collection de la Direction des Études et Recherches d'Électricité de France, no 67, éd. 1997

[3] Ouvrage collectif ISF.– *L'état de l'art dans le domaine de la fiabilité humaine*. Éd. Octarès. 1994.

Publications de l'Institut de Sûreté de Fonctionnement (ISF)

[4] Rapport *Les APR appliquées aux transports terrestres guidés*.

[5] Plaquette AMDEC.

Dans les Techniques de l'Ingénieur Traité L'Entreprise industrielle

[6] MORTUREUX (Y.). – *La sûreté de fonctionnement: démarches pour maîtriser les risques*. CD-Rom Sécurité/Prévention des risques, SE1 020 (à paraître en 2002).

[7] VEROT (Y.). – *Retours d'expérience dans les industries de procédés*. AG 4 610, Juillet 2001.