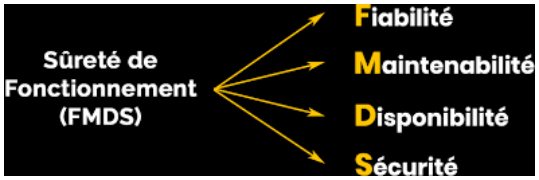
Sûreté de fonctionnement des systèmes 1

HSI M1



Dr. BACHA Sidali UFMC-1- DGT

02/04/2022
2021-2022

Table des matières

Introduction à la sûreté de fonctionnement

I

1. Objectifs du chapitre II

A la fin de ce chapitre, l'étudiant sera capable de :

- Traiter les questions de la sûreté de fonctionnement en fonction de ses attributs FMDS ;*
- Modéliser la fiabilité et la disponibilité d'un système complexe se caractérise par ses propres conditions ;
- Optimiser la disponibilité d'un système en faisant varier les conditions de fonctionnement et de maintenabilité ;
- Évaluer une situation de danger en proposant les recommandations appropriées ;

2. Qu'est-ce que la sûreté de fonctionnement

Rappel

La sûreté de fonctionnement est apparue comme une nécessité au cours du XX^{ème}, notamment avec la révolution industrielle. Le terme **dependability** est apparu dans une publicité sur des moteurs Dodge Brothers dans les années **1930**. L'objectif de la sûreté de fonctionnement est d'**atteindre le parfait de la conception de système** : zéro accident, zéro arrêt, zéro défaut (et même zéro maintenance). Pour pouvoir y arriver, il faudrait tester toutes les utilisations possibles d'un produit pendant une grande période ce qui est **impensable et impossible** dans le contexte industriel. La sûreté de fonctionnement est un domaine d'activité qui propose des moyens pour augmenter la fiabilité et la sûreté des systèmes dans des délais et avec des coûts raisonnables.

Définition

La sûreté de fonctionnement est souvent appelée la **science des défaillances** ; elle inclut leur **connaissance**, leur **évaluation**, leur **prévision**, leur **mesure** et leur **maîtrise**. Il s'agit d'un domaine transverse qui nécessite une connaissance globale du système comme les conditions d'utilisation, les risques extérieurs, les architectures fonctionnelle et matérielle, la structure et fatigue des matériaux. Beaucoup d'avancées sont le fruit du retour d'expérience et des rapports d'analyse d'accidents.

Au cours du temps, la SDF* a connu plusieurs définitions à savoir :

- La sûreté de fonctionnement d'un système informatique est la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre*.
- La sûreté de fonctionnement (dependability, SdF) consiste à évaluer les risques potentiels, prévoir l'occurrence des défaillances et tenter de minimiser les conséquences des situations catastrophiques lorsqu'elles se présentent. Elle traduit aussi la confiance qu'on peut accorder à un système.

Il existe de nombreuses définitions, de standards (qui peuvent varier selon les domaines d'application - nucléaire, spatial, avionique, automobile, etc.). On peut néanmoins considérer que le Technical Committee 56 Dependability de l'International Electrotechnical Commission (IEC) développe et maintien des standards internationaux reconnus dans le domaine de la sûreté de fonctionnement. Ces standards fournissent les méthodes et outils d'analyse, d'évaluation, de gestion des équipements, services et systèmes tout au long du cycle de développement.

3. Bref historique

Le tableau suivant présente un bref historique de la sûreté de fonctionnement.

Période	Accidents
○Jusqu'aux années 30 ➢Approche intuitive : renforcer l'élément le plus faible ➢Premiers systèmes parallèles et redondants ➢Approche statistique, taux de défaillance ➢Premières estimation de probabilité d'accidents d'avion ➢Pugsley : premier objectif de safety « taux d'accident d'avion ≤ 10−5 per flight hour »	Explosion poudrière (1794) Accident chemin de fer (1842) Titanic (1912). . .
○Années 40 ➢Analyse des missiles allemands V1 (Robert Lusser) ➢ Loi de Murphy "If anything can go wrong, it will" ➢Quantification de la disponibilité.	
○Années 50 ➢Advisory Group on Reliability of Electronic Equipment (AGREE) : •Réduction des couts de maintenance •Augmentation de la fiabilité - MTBF	Tcheliabinsk 40 (1957)
○Années 60 ➢Analyses des modes de défaillance et de leurs effets ➢Programmes de recherche spatiaux ➢Arbre de défaillance (missile Minuteman) ➢Arbres des causes (Boeing - NASA) ➢Livres sur la fiabilité (ex. Barlow and Proschan)	Torrey Canyon (1967)
○Années 70 ➢Analyse des risques ➢Collecte de données REX	
○Années 80 à nos jours ➢Nouvelles techniques (simulation, réseaux de Petri..)	Tchernoby1 (1986) Ariane V (1996) DART (NASA, 2005) Vol Rio Janeiro. . .

Cf. "Vidéo pédagogique Introduction à la Sûreté de Fonctionnement (Bref historique)"

4. Fondements de la sûreté de fonctionnement

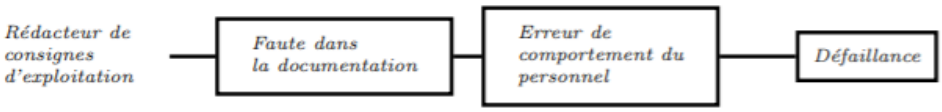
4.1. Entraves

Définition

Les entraves représentent les événements qui peuvent affecter la sureté de fonctionnement du système. Elles peuvent se diviser en trois (03) notions principales:

- La faute : La cause de l'erreur est une faute (par exemple un court-circuit sur un composant, une perturbation électromagnétique ou une faute de développement logiciel).
- L'erreur : La cause de la défaillance est une erreur affectant une partie de l'état du système (par exemple, une variable erronée).
- La défaillance : Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise

Exemple



4.2. Attributs (FMDS)

4.2.1. Fiabilité

Définition

La fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données pendant une durée donnée. La fiabilité est la continuité de service.

4.2.2. Maintenabilité

Définition

Dans les conditions données d'utilisation, la maintenabilité (Maintainability) est l'aptitude d'une entité à être maintenue ou rétablie, sur un intervalle de temps donné dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits. La maintenabilité est la capacité d'un système à **revenir** dans un état de fonctionnement correct après modifications et réparations.

4.2.3. Disponibilité

a) Aspect qualitatif de la disponibilité

Définition

La disponibilité (Availability) est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné ou pendant un intervalle de temps donné, en supposant que la fourniture des moyens extérieurs nécessaires soit assurée. La disponibilité est le fait d'être prêt au service.

[cf. Poly-FIA-MAINT-DISPAvril2014]

b) Exercice

[solution n°1 p.19*]*

La disponibilité se distingue de la fiabilité par :

- ☐ Sa capacité de calculer sa valeur de disponibilité en un instant donné
- ☐ Sa capacité à faire intégrer la maintenabilité dans ses calculs
- ☐ Sa capacité de modéliser le comportement dynamique du système

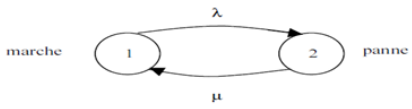
c) Chaine de Markov (Andrei Markov)

i Application à la S.D.F (1950)

Méthode

Tous les systèmes dont l'état de fonctionnement **futur** ne dépend que de l'état **présent** peuvent être décrits par un processus de Markov et en particulier, ceux pour les lesquels les probabilités de transition entre 2 états quelconques ne sont pas affectés par le temps. Il est alors homogène*. C'est le cas de tous les phénomènes à distribution **exponentielle** (i.e. taux de défaillance λ et taux de réparation μ constants)*.

Chaque sommet représente un état du système et chaque arête une transition ij valuée par le taux de transition aij.



Fondamental : Termes utilisés dans les équations générales des probabilités d'états

Probabilités :

P (i, t) être dans l'état Ei à l'instant t

P (i+1 → i, t) = μ dt naissance (réparation) entre t et t + dt

P (i-1 → i , t) = λ dt défaillance entre t et t + dt

Si à l'instant (t + dt), S est dans Ei cela suppose :

	à t	avec proba	et entre t et t + dt
1°)	E_{i-1}	$P_{i-1}(t)$	1 défaillance (proba : λ dt)
			0 naissance (proba : 1 - μ dt)
ou 2°)	E_i	$P_i(t)$	0 défaillance (proba : 1 - λ dt)
			0 naissance (proba : 1 - μ dt)
ou 3°)	E_{i+1}	$P_{i+1}(t)$	0 défaillance (proba : λ dt)
			1 naissance (proba : μ dt)

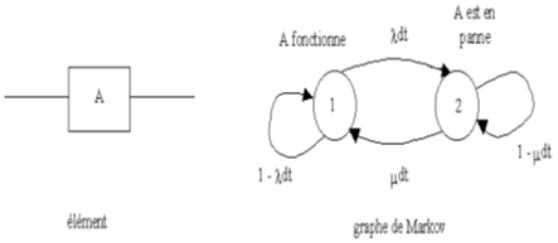
Rappel

Il est à noter que, dans la sûreté de fonctionnement, l'évaluation de la disponibilité asymptotique* se base sur deux règles principales, à savoir :

- La somme des probabilités est égal à 1 ($\Sigma P_i=1$) ;
- La somme des dérivées est égal à 0 ($\Sigma P'_i=0$) ;

Exemple

On considère le système simple à deux états



On cherche à quantifier la disponibilité asymptotique du système A.

- P1(t + dt) = P1(t).(1- λdt)+ P2 (t). μdt
- P2 (t + dt) = P2(t).(1- μdt)+ P1(t). λdt

Sous forme **matricielle**, on obtient :

$$(P_1(t+dt)\,P_2(t+dt)) = (P_1(t)\,P_2(t)) * \begin{pmatrix} 1-\lambda\,dt & \lambda\,dt \\ \mu\,dt & 1-\mu\,dt \end{pmatrix}$$

P(t + dt) = P(t)*M où

$$M = \begin{pmatrix} 1-\lambda\,dt & \lambda\,dt \\ \mu\,dt & 1-\mu\,dt \end{pmatrix}$$

est la matrice des probabilités qui caractérise le système.

On développe et on ordonne :

$$\frac{d\,P_1}{dt} = \lim_{dt\to 0} P_1(t+dt) - P_1(t)/dt = -\lambda\,P_1(t) + \mu\,P_2(t)$$

$$\frac{d\,P_2}{dt} = \lim_{dt\to 0} P_2(t+dt) - P_2(t)/dt = \lambda\,P_1(t) - \mu\,P_2(t)$$

La somme des deux dérivées est égale à 0.

Sous forme matricielle, on obtient :

$$\left(\frac{dP_1(t+dt)}{dt}\,\frac{dP_2(t+dt)}{dt}\right) = (P_1(t)\,P_2(t)) * \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix}$$

$$Q = \begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix}$$

Avec Q est la matrice de transition. Cette nouvelle matrice des taux de transition Q peut être construite aisément suivant le principe :

Vers l'Etat 1	Vers l'Etat 2		La somme des probabilités
$-\lambda$	λ	De l'Etat 1	de chaque ligne est
μ	$-\mu$	De l'Etat 2	toujours nulle

on donne le système d'équations suivantes :

$$\frac{d P_1}{dt} = -\lambda P_1 + \mu P_2 = 0$$

$$\frac{d P_2}{dt} = \lambda P_1 - \mu P_2 = 0$$

Le système devient un système d'équation à deux inconnues. Pour sa résolution, on doit trouver une deuxième équation :

$P_1+P_2=1$;

$-\lambda P_1+\mu P_2=0$;

$$p_1 = \frac{1}{1+\frac{\lambda}{\mu}} \; et \; p_2 = \frac{\lambda}{\lambda+\mu}$$

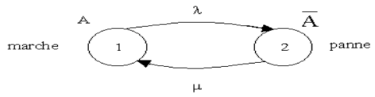
$$A_\infty = D = \frac{\mu}{\mu+\lambda}$$

ii Architectures

ii Système à 1 entité

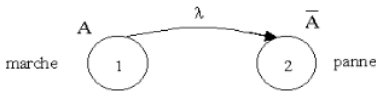
Méthode

En appelant A l'entité en état de marche et son complémentaire ($\overline{A}$)* l'entité en état de panne, on obtient dans le cas du calcul de la disponibilité le graphe de Markov suivant :



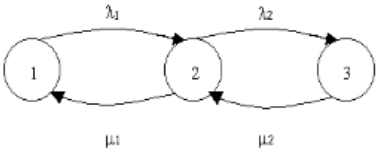
Disponibilité : A(t) = P1(t) = 1- P2(t) ; Système à 2 états (disponibilité) .

En rendant l'état 2 absorbant on obtient le graphe de Markov pour le calcul de la fiabilité :

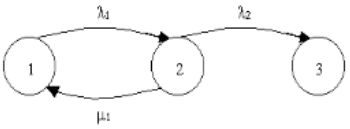


Fiabilité : R(t) = P1(t) = 1- P2(t) ; Système à 2 états (fiabilité).

Si on considère les 3 états : marche, marche dégradée, panne, on obtient dans le cas du calcul de la disponibilité le graphe de Markov suivant :

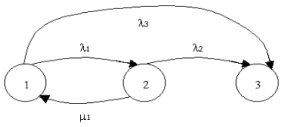


A(t) = P1(t) + P2(t) = 1- P3(t) ; Système à 3 états (disponibilité).



R(t) = P1(t) + P2(t) = 1- P3(t) ; Système à 3 états (fiabilité).

Un système à 3 états avec défaillance catastrophique direct (fiabilité) se donne comme suit :



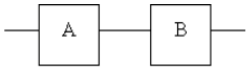
R(t) = P1(t) + P2(t) = 1- P3(t).

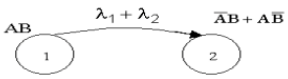
ii Système à 2 entités:

Méthode : Dispositifs non réparables

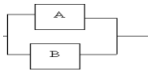
- **Série**

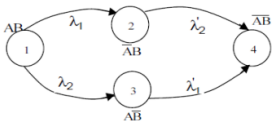
Système à 2 entités:





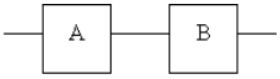
- **Parallèle**

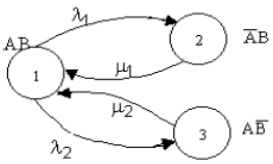




Méthode : Dispositifs réparables

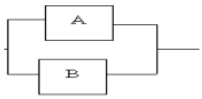
- **Série**

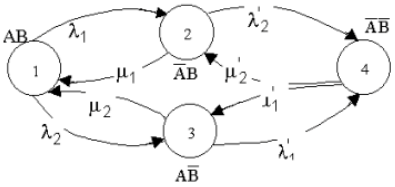




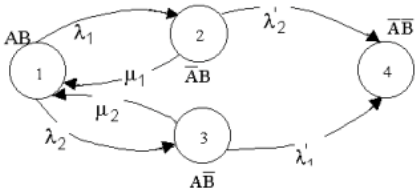
- **Parallèle**

Graphe relatif à la disponibilité.





Le graphe relatif à la fiabilité se donne comme suit :



Complément

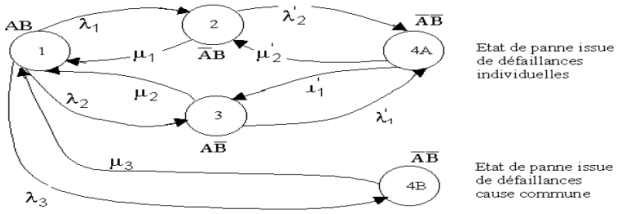
Cause commune

On considère un système à 2 entités en parallèle avec une défaillance de type cause commune. Cette cause commune entraîne une défaillance catastrophique des deux entités simultanément.

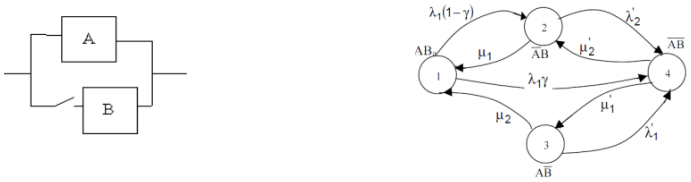
- **Pour un dispositif non réparable :**

- **Pour un dispositif non réparable :**

Si le temps de réparation (TTR) du système pour passer de l'état 4 vers l'état 1 est **différent** après la défaillance **cause commune** et **après les défaillances individuelles** alors le programme de réparation **dépend du passé** ce qui contre dit la propriété de **non-mémoire** du modèle. Nécessité d'avoir 2 états de panne 4A et 4B :



Dans le cas de deux entités en redondance passive, le graphe de Markov se donne comme suit :



Remarque

Politique mono ou bi-réparateur ou mettre une machine identique en parallèle. Une politique mono ou bi-réparateur signifie que pour chaque panne nous pouvons calculer la MTTR donc nous pouvons déterminer μ. La politique mono–réparateur, implique l'application d'un taux de réparation **normalisé**. Pour une politique bi-réparateur, il faut affecter μ d'un coefficient **2**:

$$2\mu = \frac{1}{MTTR}$$

Concrètement, en quoi consiste la division de la MTTR par 2 ?

Soit :

- En doublant l'effectif pour la réparation ;
- En mettant à la disposition de l'équipe de réparation des moyens plus performants, etc.

Maintenant, le graphe de Markov est utilisé dans plusieurs domaines tels que le transport, la sécurité des équipements,etc*.

ii Exercice

[solution n°2 p.19*]*

Afin d'évaluer correctement la disponibilité d'un système, on doit respectivement suivre les étapes suivantes :

Résoudre le système d'équation

Construire la matrice de transition

Déduire la disponibilité du système

Schématiser le graphe de Markov associé

4.2.4. Sécurité

La gestion des risques est le processus par lequel les organisations traitent méthodiquement les risques qui s'attachent à leurs activités et cherchent des bénéfices durables dans le cadre de ces activités. La gestion du risque est centrée sur l'identification et le traitement des risques. La **sécurité** est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques*.

Afin d'assurer l'application de processus d'analyse du risque, plusieurs méthodes d'analyse des risques peuvent s'utiliser, à savoir :

- L'APR;
- L'AMDEC;
- L'ADD;
- L'ADE;
- La HAZOP ....etc*.

a) Approches déductives et inductives d'analyse des risques

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**. 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**.

i Analyse (Management) préliminaire des risques

Définition

L'analyse Préliminaire de Risque (Danger) a été développée au début des années 1960 dans les domaines aéronautique et militaire. Le but consiste à identifier les entités dangereuses d'un système, puis à regarder pour chacune d'elles comment elles pourraient générer un incident ou un accident plus ou moins grave suite à une séquence d'événements causant une situation dangereuse.

Il s'agit d'une méthode inductive, qualitative, systématique et assez simple à mettre en œuvre. Concrètement, l'application de cette méthode réside dans le renseignement d'un tableau en groupe de travail pluridisciplinaire*.

Méthode

Les étapes de la méthode APR peuvent se résumer dans ce tableau :

1	2	3	4	5	6	7	8
Système ou fonction à étudier	Produit ou équipement	Situation de danger	Causes	Conséquences	Sécurités existantes	Propositions d'améliorations	Observation

Attention

- La colonne n°3 désigne l'événement **Redouté Central** (situation de danger). Par exemple, la mise en suspension de poussières, la fuite de gaz ou l'inflammation de matières combustibles.
- La colonne n°4 désigne l'événement **Initiateur** (cause de la situation de danger). Un Événement Redouté Central peut avoir plusieurs Événements Initiateurs, aussi bien internes (défaillance mécanique, erreur humaine, ...) qu'externes (effets dominos, ..).
- La colonne n°5 désigne les Phénomènes dangereux susceptibles de découler de l'événement
- Redouté Central (ex : explosion, incendie, pollution des eaux superficielles, etc.);
- La colonne n°6 présente, pour les scénarios identifiés, les principales barrières de sécurité indépendantes La distinction entre les barrières de protection et de prévention est réalisée sous la forme de 2 sous-colonnes.
- La colonne n°8 comprend les éventuelles observations ou remarques relatives au scénario considéré.

Pour identifier les entités et les situations dangereuses susceptibles d'en découler, l'analyste est aidé par des listes de contrôles (check-lists) d'entités dangereuses, de situations dangereuses et d'événements redoutés.

Ces check-lists sont spécifiques au domaine d'étude concerné.

Exemple : Exemple d'une Check liste

Electrique :

- Eléctrocution ;
- Brulure ;
- Coupure de courant ;
- Arc électrique.

Mécanique :

- Chute élément lourd ;
- Écrasement ;
- Projection d'éléments ;

Équipements sous-pression :

- Surpression ;
- Cavitation ;
- Défaut position clapet de surpression.

Conseil

Afin de savoir la pertinence et l'efficacité de l'APR, il est recommandé de se référer à ses avantages et inconvénients.

Avantages

- Permettre un examen relativement rapide des situations dangereuses sur des installations.
- Ne nécessite pas un niveau de description du système étudié très détaillé.

Inconvénients

- L'APR ne permet pas de caractériser finement l'enchaînement des évènements susceptibles de conduire à un accident majeur pour des systèmes complexes ;
- Nécessite une étude plus détaillée;
- Absence de combinaison entre les causes;

ii Analyse des modes de défaillances, de leurs effets et leurs criticités AMDE(C)

Définition

L'AMDEC* a été crée aux Etats-Unis par la société Mc Donnell Douglas en 1966. D'après AFNOR, L'analyse des **modes de défaillance** de leurs **effets** et de leur **criticités** (AMDEC) est une méthode inductive permettant pour chaque composant d'un système, de **recenser** son mode de défaillance et son effet sur le fonctionnement ou sur la sécurité du système.

Il existe plusieurs types d'AMDEC, à savoir:

- **AMDEC PROCESSUS :**

Analyse des opérations de Production pour améliorer la QUALITE de FABRICATION du produit. Ex: Défaut observable sur la pièce fabriquée

- **AMDEC MOYEN DE PRODUCTION (machines, systèmes) :**

Analyse de la Conception et /ou de l'Exploitation des Équipements de Production pour améliorer leur DISPONIBILITÉ. Ex: Fonction : absente; dégradée; arrêtée.

- **AMDEC PRODUIT:**

Analyse de la Conception d 'un produit pour améliorer sa QUALITE et sa FIABILITE. Ex: Les critères déterminés ne sont pas atteints.

- **AMDEC SECURITE :**

Analyse des défaillances et des Risques prévisionnels sur un équipement pour améliorer la Sécurité et la FIABILITE*.

L'AMDEC est une démarche à la fois **qualitative** et **quantitative** :

QUALITATIVE

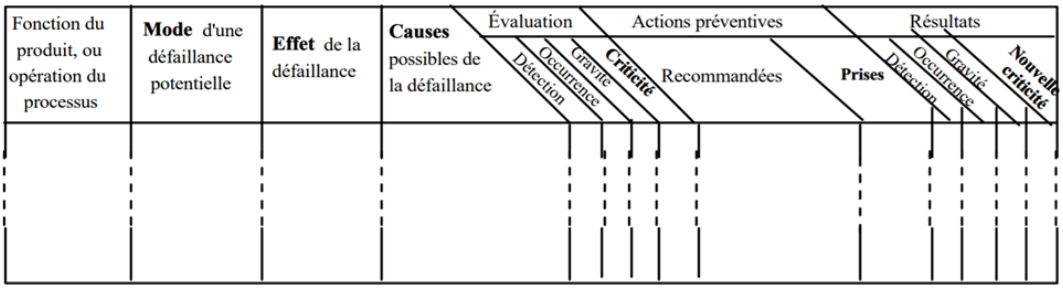
- Découpage Fonctionnel.
- Analyse des Modes de Défaillances.
- Analyse des Causes.
- Analyse des Effets.

QUANTITATIVE

- Cotation de paramètres (Fréquence d 'apparition , Gravité ....).
- Calcul de la Criticité à partir de ces paramètres.
- Mesure des résultats.

Méthode

Les résultats de l'AMDEC peut être regroupés dans un tableau comme il est montré dans la figure ci-dessous :



Remarque

Un mode de défaillance est la manière dont le système peut s'arrêter de fonctionner ou fonctionner anormalement. Le mode de défaillance est relatif à chaque fonction de chaque élément. Il s'exprime en termes physiques.

Exemples : rupture, coupure d'électricité, coincement, fuite...

Complément

Comme toute autre méthode, on doit savoir les points forts (avantages) et faibles (inconvénients ou limites) de la méthode AMDEC.

Points forts :

Outil très performant lorsqu'il est utilisé dès la phase de conception ;

Connaissance des **états dégradés** du système ;

Outil de base pour la construction du plan de maintenance.

Points faibles :

Lourdeur de gestion pour des systèmes complexes (beaucoup de composants, multiples fonctions, plusieurs modes opératoire...) ;

L'AMDEC ne met pas en évidence les combinaisons éventuelles de défaillances, entraînant la défaillance globale du système ;

Volume d'information très important et souvent non homogène.

ii Exercice : Autour du mot "mode de défaillance"

[solution n°3 p.19*]*

Un mode de défaillance peut prendre des événements tels que:

- ☐ La surpression ;
- ☐ La corrosion ;

- ☐ L'erreur humaine ;
- ☐ La faute ;
- ☐ La fuite ;
- ☐ La rupture
- ☐ Coincement ;

Solutions des exercices

> **Solution** n°1

Exercice p. 7

La disponibilité se distingue de la fiabilité par :

- [x] Sa capacité de calculer sa valeur de disponibilité en un instant donné
- [x] Sa capacité à faire intégrer la maintenabilité dans ses calculs
- [ ] Sa capacité de modéliser le comportement dynamique du système

> **Solution** n°2

Exercice p. 13

Afin d'évaluer correctement la disponibilité d'un système, on doit respectivement suivre les étapes suivantes :

Schématiser le graphe de Markov associé | Construire la matrice de transition

Résoudre le système d'équation | Déduire la disponibilité du système

> **Solution** n°3

Exercice p. 17

Un mode de défaillance peut prendre des événements tels que:

- [x] La surpression ;
- [ ] La corrosion ;
- [ ] L'erreur humaine ;
- [ ] La faute ;
- [x] La fuite ;
- [x] La rupture
- [x] Coincement ;

Glossaire

Complémentaire

Se lit "A bar" et représente l'événement contraire de A.

Disponibilité asymptotique

Après certains temps de fonctionnement,le système retrouve sa valeur de disponibilité asymptotique (moyenne) à un instant t= ∞.

Homogène

Cette homogénéité concerne les systèmes dont la probabilité d'occurrence d'un événement est proportionnelle à la longueur d'un petit intervalle et indépendante du temps d'occurrence de l'événement lui-même, c'est la notion de stationnarité.

Inconvénient

C'est cette propriété du processus markovien qui représente son inconvénient majeur en rendant la modélisation indépendante du milieu extérieur du système.

Abréviations

AMDEC : Analyse des modes de défaillances, de leurs effet et leurs criticités.

FMDS : Fiabilité-Maintenabilité-Disponibilité-Sécurité

SDF : Sûreté de fonctionnement

Références

AFNOR, AMDEC guide pratique, no. 2. 2011. Guide pratique

INERIS-DRA-2006-P46055-CL47569 : Méthodes d'analyse des risques générés par une installation industrielle. Méthodes d'analyse des risques

J.C. Laprie et al., Guide de la sûreté de fonctionnement, Cépaduès, 1996, 380 p. Guide de la sûreté de fonctionnement

J. W. Vincoli, "Preliminary Hazard Analysis," in Basic Guide to System Safety, John Wiley & Sons, Ltd, 2014, pp. 71–90. Preliminary Hazard Analysis

JEAN-CLAUDE LIGERON et al, Modélisation de la disponibilité d'un système de transports par chaînes de Markov,Revue de statistique appliquée,Vol.8, N°3,1980,P. 45-68 Modélisation de la disponibilité d'un système de transports par chaînes de Markov

Villemeur, A. (1997). Sûreté de fonctionnement des systèmes industriels. Direction des études et recherches d'Electricité de France. Eyrolles, 1ère édition. ISBN 978-2-212-01615-4 Sûreté de fonctionnement des systèmes industriels