Agl: chapitre 1

1 composant

Un système est constitué de composants.Un composant est une machine abstraite dont l'état est modifié par certains phé-nomènes. Ceux-ci proviennent soit de l'environnement soit du composant lui-même;dans le premier cas on les appelle, en général, des événements et dans le second cas,des actions du composant.

2 risque

Le risque peut se définir comme la survenue d'un évènement imprévu, plus ou moins nocif, fautif ou non, pouvant causer un dommage. Le préjudice subi peut faire l'objet d'une réparation, sous la forme d'une indemnisation. I1 se caractérise par sa nature, sa probabilité de survenue, sa gravité

3 Défaillance

Définition de la défaillance selon la norme NF X60 –011 : *"altération ou cessation d'un bien à accomplir sa fonction requise ."*

Synonymes usuels non normalisés : *"failure"* (anglais), dysfonctionnement, dommages, dégâts, anomalies, avaries, incidents, défauts, pannes, détériorations. Une défaillance peut être :

- Partielle: s'il y a altération d'aptitude du bien à accomplir sa fonction requise.
- Complète: s'il y a cessation d'aptitude du bien à accomplir sa fonction requise.
- Intermittente: si le bien retrouve son aptitude au bout d'un temps limité sans avoir subi d'action corrective externe.

4 Les modes de défaillances

Le mode de défaillance est la façon dont un produit, un composant, un ensemble, un processus ou une organisation manifeste une défaillance ou s'écarte des

spécifications. Voici quelques exemples pour illustrer cette définition:

- déformation;
- vibration;
- coincement;
- desserrage;
- corrosion;
- fuite;
- perte de performance;
- court-circuit;
- flambage;
- ne s'arrête pas;
- ne démarre pas;
- dépasse la limite supérieure tolérée, etc.

5 Arbres de défaillances

La méthode de l'arbre de défaillances, encore appelée arbre des causes (fault tree) est née en 1962 dans la société Bell Telephone grâce à Watson qui travaillait sur le projet Minuteman. Dans les années suivantes, les règles de construction ont été formalisées par Haasl en 1965, par l'University of Washington et Boeing. Dans les années 70, Vesely a jeté les bases de l'évaluation quantitative, Kinetic Tree Theory (KITT). Enfin, en 1992, la dernière grande avancée est due à Coudert, Madre et Rauzy qui les ont codés avec des Diagrammes de décision binaires (DDB) obtenant ainsi une grande efficacité de calcul. Cette méthode a pour objectif de déterminer les combinaisons possibles d'événements qui entraînent l'occurrence d'un événement indésirable (ou redouté). L'idée est de représenter graphiquement la logique de dysfonctionnement d'un système.

6 Analyse qualitative et quantitative

L'aspect qualitatif de l'étude consiste à recenser les défaillances potentielles des fonctions du système étudié, de rechercher et d'identifier les causes des défaillances et d'en connaître les effets qui peuvent affecter les clients, les utilisateurs et l'environnement interne ou externe.

L'aspect quantitatif consiste à estimer le risque associé à la défaillance potentielle. Le but de cette estimation est l'identification et la hiérarchisation des défaillances potentielles. Celles- ci sont alors mises en évidence en appliquant

certains critères dont, entre autres, l'impact sur le client. La hiérarchisation des modes de défaillance par ordre décroissant, facilite la recherche et la prise d'actions prioritaires qui doivent diminuer l'impact sur les clients ou qui élimineraient complètement les causes des défauts potentiels.

7 AMDE

La méthode de Analyse des Modes de Défaillances et de leurs Effets (AMDE) est une des premières méthodes systématiques permettant d'analyser les défaillances. Elle a été développée par l'armée américaine et se trouve dans la première guideline Military Procedure MIL-P-1629 "Procedures for performing a failure mode, effects and criticality analysis" du 9 novembre 1949. Cette analyse est largement utilisée pendant les phases initiales de développement. Une AMDE (FMEA pour Failure Mode and Effects Analysis) est une analyse détaillée de toutes les défaillances simples, de leurs conséquences (ainsi qu'un chiffrage préliminaire de probabilité d'occurrence). Elle permet d'identifier les éléments critiques de sécurité (provoquant des événements critiques ou catastrophiques) ainsi que les fautes dormantes. En résumé, une AMDE permet :

1. identifier les modes de défaillances des différentes parties du système,
2. d'évaluer les effets de chaque mode de défaillance des composants sur les fonctions du système,
3. d'identifier les modes de défaillances qui auront un effet important sur la sécurité, la fiabilité, la sécurité . . .

Procédure

1. Définir le système à analyser
   - Les missions et fonctions principales du système
   - Conditions opérationnelles et environnementale
2. Collecter les informations disponibles qui décrivent le système (incluant schémas, spécifications, listes de composants, . . .) et collecter les informations sur les précédents conceptions similaires.
3. Préparer les rapports AMDE.

8 AMDEC

L'AMDEC, analyse des modes de défaillance, de leurs effets et de leur criticité, est un outil d'analyse performant qui permet de recenser de manière exhaustive les risques de dérive d'un processus, d'un produit ou d'un moyen de production. Elle s'inscrit dans la logique de maîtrise des risques ; sa finalité est de mettre en place des plans d'actions préventives visant à éliminer ou réduire les risques

liés à la sécurité de l'utilisateur, au non qualité, à la perte de productivité, à l'insatisfaction des clients . L'AMDEC se définit comme une " *méthode inductive d'analyse de système utilisée pour l'analyse systématique des causes, des effets des défaillances qui peuvent affecter les composants de ce système* ". Cette méthode est systématique, participative et préventive.

L'AMDEC a pour objectif, dans une démarche inductive rigoureuse, d'identifier les défaillances dont les conséquences peuvent affecter le fonctionnement d'un système et de les hiérarchiser selon leur niveau de criticité afin de les maitriser. On obtient en sortie l'ensemble des dysfonctionnements potentiels associes a leur criticité (fréquence d'apparition, gravite des effets et probabilité de détection de la défaillance) ainsi que les plans d'actions a mettre en œuvre afin de diminuer la criticité en faisant varier un des trois facteurs.

- Types de l'AMDEC :

Il existe plusieurs types de la méthode d'analyse :

- L'AMDEC organisation
- L'AMDEC-Produit
- L'AMDEC-Processus
- L'AMDEC moyen
- L'AMDEC service
- L'AMDEC sécurité

9 La sûreté de fonctionnement

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 systéme 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.

La sûreté de fonctionnement d'un systéme informatique est la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre. Elle consiste à évaluer les risques potentiels, prévoir l'occurrence des défaillances et tenter de minimiser les conséquences des situations catastrophiques lorsqu'elles se présentent.

10 Analyses préliminaires à la sûreté de fonctionnement

10.1 L'analyse fonctionnelle

Le but de l'analyse fonctionnelle est de déterminer d'une manière assez complète les fonctions principales d'un produit, les fonctions contraintes et les fonctions élémentaires.

1. Les fonctions principales : sont les fonctions pour lesquelles le système a été conçu, donc pour satisfaire les besoins de l'utilisateur.
2. Les fonctions contraintes : répondent aux interrelations avec le milieu extérieur.
3. Les fonctions élémentaires : assurent les fonctions principales, ce sont les fonctions des différents composants élémentaires du système.

Pour réaliser correctement l'analyse fonctionnelle il faut effectuer trois étapes principales :

- Définir le besoin à satisfaire. Le principe consiste à décrire le besoin et la façon dont il est satisfait et comment il risque de ne pas être satisfait.
- Définir les fonctions qui correspondent au besoin.
- Etablir l'arbre fonctionel afin de visualiser l'anlyse fonctionnelle. Très souvent les fonctions principales comportent des sous-fonctions ou résultent d'un ensemble des fonctions élémentaires. D'où le besoin de l'arbre fonctionnel .

10.2 APR

L'APR (analyse préliminaire des risques) est une méthode couramment utilisée dans le domaine de l'analyse des risques. Il s'agit d'une méthode inductive, 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.

Objectif

L'APR a pour objectif principal d'identifier les scénarios d'accident majeurs et les mesures de sécurité qui empêchent ces scénarios de se produire ou en limitent les effets. Pour cela, tous les scénarios d'accident potentiels ainsi que leur causes, les conséquences possibles de ces événements et les mesures de sécurités existantes seront analysés.

11 Méthodes d'analyse de sûreté de fonctionnement

Une analyse prévisionnelle de sûreté de fonctionnement est un processus d'étude d'un système réel de fa¸con à produire un modèle abstrait du système relatif à une caractéristique de sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité, sécurité). Les éléments de ce modèle seront des événements susceptibles de se produire dans le système et son environnement, tels par exemple :

- des défaillances et des pannes des composants du système,
- des événements liés à l'environnement,
- des erreurs humaines en phase d'exploitation.

Le modèle permet ainsi de représenter toutes les défaillances et les pannes des composants du système qui compromettent une des caractéristiques de SdF. Afin d'aider l'analyste, plusieurs méthodes d'analyse ont été mises au point. Les principales sont :
APD Analyse Préliminaire des Dangers,
AMDE Analyse des Modes de Défaillances et de leurs Effets,
MDS Méthode du Diagramme de Succès,
MTV Méthode de la Table de Vérité,
MAC Méthode de l'Arbre des Causes,
MCPR Méthode des Combinaisons de Pannes Résumées,
MACQ Méthode de l'Arbre des Conséquences,
MDCC Méthode du Diagramme Causes-Conséquences,
MEE Méthode de l'Espace des Etats.

12 Diagramme de fiabilité

Historiquement, la méthode du diagramme de fiabilité ou de succès est la première à avoir été utilisée pour analyser les systèmes. Ses limites sont rapidement apparues, néanmoins elle permet de modéliser rapidement le système. On suppose dans la suite que le système n'est pas réparable.

Un diagramme de fiabilité est défini par :

- Une entrée E, un corps de diagramme et un sortie S
- Un flux est transmis de E jusqu'à S en passant par les différents chemins.
- Défaillance d'une entité arrête le flux au niveau du composant.
- S'il n'existe pas de chemin jusqu'à S, le système est défaillant, sinon il fonctionne.
- Configuration série ou/et parallèle.

13 Chaînes de Markov

La Méthode de l'Espace d'Etat (MEE) a été développée pour l'analyse de sûreté de fonctionnement de système réparable. Les arbres de défaillances, vus dans le chapitre précédent, permettent de bonnes descriptions statiques de système mais ne prennent pas en compte les reconfigurations, comme les réparations. Les premières utilisations des processus stochastiques dans les années 50 utilisaient des processus markoviens ; des généralisations ont ensuite été faites. Dans cette partie nous nous concentrons sur les processus markoviens. Andrei Markov a publié ses premiers résultats en 1906, qui ont ensuite été généralisés à un espace d'états infini dénombrable par Andrei Kolmogorov en 1936.

Un processus stochastique est un ensemble de variables aléatoires (Xt)t ≥ 0

à valeurs dans l'ensemble des observations. Un processus est markovien si la probabilité de passage de l'étape présente à la suivante ne dépend pas du passé, i.e.

$$\mathrm{P}(\mathrm{X}_t \epsilon A | X_{tn} \epsilon A_n, ..., X_1 \epsilon A_1) = P(X_t \epsilon A | X_{tn} \epsilon A_n)$$

14 Réseaux de Petri

Ces réseaux présentent des caractéristiques intéressantes telles que la modélisation et la visualisation de comportements parallèles, de la synchronisation et partage de ressources. De plus leurs aspects théoriques ont été largement étudiés et les résultats théoriques les concernant sont très abondant.

C'est un outil de modélisation utilisé généralement en phase préliminaire de conception de système pour leur spécification fonctionnelle, modélisation et évaluation.

Les principaux utilisateurs de ces réseaux sont les informaticiens et les automaticiens. Cependant c'est un outil assez général pour modéliser des phénomènes très variés. Il permet notamment : la modélisation des systèmes informatiques, l'évaluation des performances des systèmes discrets, des interfaces homme-machine, la commande des ateliers de fabrication, la conception de systèmes temps réel, la modélisation des protocoles de communication, la modélisation des chaines de production (de fabrication) ...