Partie N°02

Sûreté de fonctionnement

1- Définition de la sûreté de fonctionnement

La Sûreté de Fonctionnement est l'aptitude d'un système à satisfaire à une ou plusieurs fonctions requises dans des conditions données

La Sûreté de fonctionnement consiste à connaître, évaluer, prévoir, mesurer et maîtriser les défaillances des systèmes technologiques et les défaillances humaines.
La Sûreté de fonctionnement est appelée la science des « défaillances ». D'autres désignations existent suivant les domaines d'applications :

analyse de risque (milieu pétrolier), aléatique, cyndinique (science du danger), FMDS (Fiabilité, Maintenabilité, Disponibilité, Sécurité), en anglais RAMS (Reliability, Availability, Maintainability and Safety) :

Fiabilité est la probabilité de non-défaillance d'un équipement sur un intervalle de temps donné

Disponibilité se définit par la probabilité d'être en état d'accomplir sa fonction à un instant donné.

Maintenabilité est l'aptitude d'un système à être maintenu en état : Elle correspond à la probabilité que la remise en état d'une entité en panne soit effectuée dans un intervalle de temps.

Sécurité implique actuellement les aspects réglementaires de la sécurité des personnes.

2- Définitions

Fiabilité R(t) (Reliability) : La fiabilité est l'aptitude d'un composant ou d'un système à fonctionner pendant un intervalle de temps. Plus précisément, la fiabilité est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, durant un intervalle de temps donné. Le terme fiabilité est également utilisé pour désigner la valeur de la fiabilité et

peut être défini comme une probabilité. C'est alors la probabilité pour qu'une entité puisse accomplir une fonction requise, dans des conditions données, pendant un intervalle de temps donné. La notion de fiabilité est associée à celle de taux de défaillance. **Maintenabilité (Maintainability) :** La maintenabilité est l'aptitude d'un composant ou d'un système à être maintenu ou remis en état de fonctionnement. Plus précisément, la maintenabilité est, dans des conditions données d'utilisation, l'aptitude d'une entité à être maintenue ou rétablie dans un état ou elle peut accomplir une fonction requise, lorsque la maintenance est accomplie dans des conditions données, en utilisant des procédures et des moyens prescrits. Le terme maintenabilité est également utilisé pour désigner la valeur de la maintenabilité. C'est alors, pour une entité donnée, utilisée dans des conditions données d'utilisation, la probabilité pour qu'une opération de maintenance active puisse être effectuée pendant un intervalle de temps donné, lorsque la maintenance est assurée dans des conditions données et avec l'utilisation de procédures et des moyens prescrits. **Disponibilité (Availability) :** La disponibilité est l'aptitude d'un composant ou d'un système à être en état de marche à un instant donné.

Plus précisément, la disponibilité est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant donné, en supposant que la fourniture des moyens nécessaires est assurée. Le terme disponibilité est également utilisé pour désigner la valeur de la disponibilité et peut être défini comme une probabilité. C'est alors la probabilité pour qu'une entité puisse accomplir une fonction requise, dans des conditions données, à un instant donné.

Sécurité (Safety) : La sécurité est l'aptitude d'une entité à ne pas conduire à des accidents inacceptables. Plus précisément, la sécurité est l'aptitude d'un produit à respecter, pendant toutes les phases de vie, un niveau acceptable de risques d'accident susceptible de causer une agression du personnel ou une dégradation majeure du produit ou de son environnement.

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

Rq : si on désigne la fonction fiabilité par R (Reliability), la fonction défaillance F (Failure) est égale à 1-R. Chez certains clients, elle peut se retrouver sous la dénomination « défiabilité ».

3- Outils utilisés en sûreté de fonctionnement

3-1 Analyse Préliminaire des Risques (APR)

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

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

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

3-2 Arbre de défaillances (ADD)

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

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

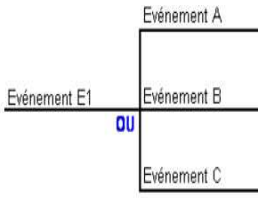
L'événement redouté (ER) est l'événement indésirable pour lequel on recherche toutes les causes, et leur combinatoire, qui y conduisent. Cet événement est unique pour un arbre de défaillances et se trouve à gauche de l'arbre (ou au sommet). Il doit être défini de façon précise afin d'éviter d'avoir une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

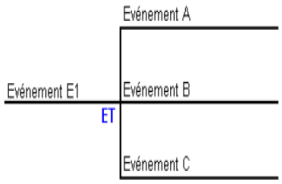
Cet événement provient généralement de l'analyse préliminaire de risques utilisée en amont de l'arbre de défaillances. **Portes logiques**

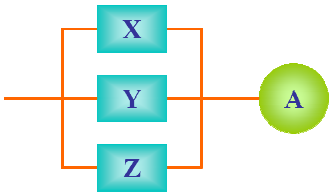
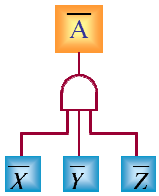
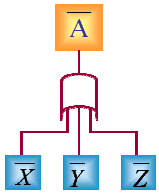
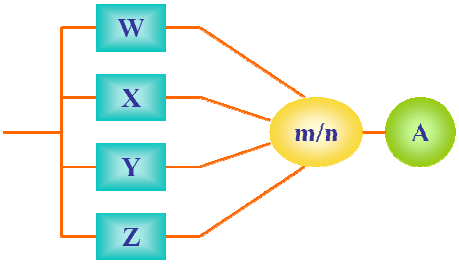
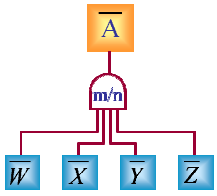
L'arbre de défaillances est particulièrement bien adapté aux événements combinatoires, mais devient délicat à mettre en œuvre quand il s'agit d'événements séquentiels.

Porte « OU » : l'événement E1 se produit dès qu'un événement A, B ou C se produit.

Porte « ET » : l'événement E1 ne se produit que si les événements A, B et C se produisent simultanément.

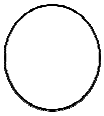




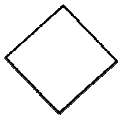
Représentation fonctionnelle	Opérateur (Dysfonctionnel)	Symbole
OU 	ET	
ET 	OU	
	COMBINAISON (m, n)	

❑ Représentations :

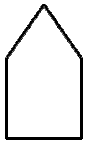
Combinaison d'événements



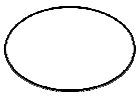
Élémentaire



Non élémentaire mais non développé
ou non développé momentanément



Case configuration



Événement conditionnel

Définitions des événements de base :

- **Élémentaire :**
  - généralement une défaillance,
  - phénomène assez connu pour ne pas le développer plus (probabilité faible - Rex).
- **Non élémentaire et non développé :**
  - événement étant une cause externe au système étudié (Ex : alimentation HS),
  - porte ET avec plus de 3 branches.
- **Non élémentaire et non développé momentanément :**
  - pas de renseignements suffisants,
  - à développer par un fournisseur ou à documenter.
- **Case configuration :**
  - Permet de réaliser un seul arbre pour différentes phases de vie.