Partie 3 : ENTRAVES, ATTRIBUTS et METHODES(Taxonomie)

La sureté de fonctionnement manipule un certain nombre de concepts que nous précisons dans cette partie en donnant des définitions précises. La sureté de fonctionnement peut être vue comme étant composée des trois éléments suivants :

Attributs : points de vue pour évaluer la sureté de fonctionnement ;
Entraves : évènements qui peuvent affecter la sureté de fonctionnement du système ;
Moyens : moyens pour améliorer la sureté de fonctionnement.

3.1 / Entraves

Commençons par détailler les entraves qui peuvent affecter le système et dégrader la sureté de fonctionnement. Les entraves sont reparties en 3 notions :

Les fautes, les erreurs et les défaillances

Les définitions sont récursives car la défaillance d'un composant est une faute pour le système qui le contient.

Définition Faute (Fault) : La cause de l'erreur est une faute (par exemple un court-circuit sur un composant, une perturbation électromagnétique ou une faute de d'développement logiciel).

Définition Erreur (Defect) : La cause de la défaillance est une erreur affectant une partie de l'état du système (par exemple, une variable erronée).

Définition Défaillance (Failure) : Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise.

Définition Panne : La panne est l'inaptitude d'une entité à accomplir une mission.
Une panne résulte toujours d'une défaillance.

Les défaillances dans un système peuvent avoir des effets différents. Certaines défaillances n'affectent pas directement les fonctions du système et ne nécessitent qu'une action corrective ; d'autres, en revanche, affectent la disponibilité ou la sécurité.

On utilise généralement une échelle de gravite des effets et on considère traditionnellement 4 catégories de défaillances.

Défaillance mineure : défaillance qui nuit au bon fonctionnement (minor) d'un système en causant un dommage négligeable au système ou a son environnement sans présenter de risque pour l'homme.

Défaillance significative : défaillance qui nuit au bon fonctionnement (major) sans causer de dommage notable ni présenter de risque important pour l'homme.

Défaillance critique : défaillance qui entraine la perte d'une (hasardeuse) (ou des) fonction(s) essentielle(s) du système et cause des dommages importants au système en ne présentant qu'un risque négligeable de mort ou de blessure.

Défaillance catastrophique : défaillance qui occasionne la perte d'une (catastrophique) (ou des) fonction(s) essentielle(s) du système en causant des dommages importants au système ou à son environnement et/ou entraine la mort ou des dommages corporels.

Définition Mode de défaillance (Failure mode) : Un mode de défaillance est l'effet par lequel une défaillance est observée. Plus, précisément, il s'agit d'un des états possibles d'une entité en panne pour une fonction requise donnée.

Classification des modes de défaillance :
On classe généralement les modes de défaillance en 4 catégories :
- Fonctionnement prématuré (ou intempestif) : Fonctionne alors que ce n'est pas prévu à cet instant
- ne fonctionne pas au moment prévu
- ne démarre pas lors de la sollicitation
- ne s'arrête pas au moment prévu continue à fonctionner alors que ce n'est pas prévu défaillance en fonctionnement

Définition Système cohérent : Un système est dit cohérent si :
- la panne de tous les composants entraine la panne du système,
- le fonctionnement de tous les composants entraine le fonctionnement du système,
- lorsque le système est en panne, aucune défaillance supplémentaire ne rétablit le fonctionnement du système,
- lorsque le système est en fonctionnement, aucune réparation n'induit la panne du système.

Nous ne considérons dans la suite que des systèmes cohérents.

3.2 / Attributs

Les attributs de la sûreté de fonctionnement sont parfois appelés FDMS pour Fiabilité, Disponibilité, Maintenabilité et Sécurité (RAMSS pour Reliability, Availability, Maintainability, Safety, Security).

La disponibilité est le fait d'être prêt au service.

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

Définition Fiabilité (Reliability) : La fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise dans des conditions données pendant une durée donnée.
La sécurité est l'aptitude à ne pas provoquer d'accidents catastrophiques.

Définition Sécurité innocuité (Safety) : La sécurité innocuité est l'aptitude d'une entité à éviter de faire apparaitre, dans des conditions données, des évènements critiques ou catastrophiques.

La maintenabilité est la capacité d'un système à revenir dans un état de fonctionnement correct après modifications et réparations.

Définition Maintenabilité (Maintainability) : Dans les conditions données d'utilisation, la maintenabilité 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.

D'autres attributs de sureté de fonctionnement ont été identifies comme par exemple la testabilité (le degré d'un composant ou d'un système à fournir des informations sur son état et ses performances), ou la diagnosticabilite (capacité d'un système à exhiber des symptômes pour des situations d'erreur) survivabilite (capacité d'un système à continuer sa mission après perturbation humaine ou environnementale) et ainsi de suite.

Les moyens

Les moyens sont des solutions éprouvées pour casser les enchainements Faute ! Erreur ! défaillance et donc améliorer la fiabilité du système.

- La prévention de faute consiste à éviter des fautes qui auraient pu être introduites pendant le développement du système. Cela peut être accompli en utilisant des méthodologies de développement et de bonnes techniques d'implantation.
- L'élimination de faute peut être divisée en 2 catégories : élimination pendant la phase de développement et élimination pendant la phase d'utilisation. Pendant la phase de développement, l'idée est d'utiliser des techniques de vérification avancées de façon a détecter les fautes et les enlever avant envoi à la production. Pendant l'utilisation, il faut tenir à jour les défaillances rencontrées et les retirer pendant les cycles de maintenance.
- La prévision de faute consiste à anticiper les fautes (de manière qualitative ou probabiliste) et leur impact sur le système.
- La tolérance aux fautes consiste à mettre en place des mécanismes qui maintiennent le service fourni par le système, même en présence de fautes. On accepte dans ce cas un fonctionnement dégrade. La tolérance aux fautes repose sur l'utilisation de mécanismes de redondance, l'idée est de réaliser la même fonction par des moyens différents.

On distingue plusieurs types de redondance :

- Redondance homogène : on réplique plusieurs composants identiques
- Redondance avec dissemblance : les sous-systèmes réalisent les mêmes fonctions mais sont différents (par exemple, plusieurs équipes de conception, matériel diffèrent).
- Redondance froide : les composants sont actifs quand ceux déjà actifs tombent en panne.
- Redondance chaude : les composants tournent en parallèle et politique de prise de main.
- Redondance tiède : les composants sont idole avant de prendre la main.

D'autres mécanismes existent comme les comparateurs ou les voteurs. L'idée est de récupérer plusieurs valeurs calculées par redondance et de déterminer quelle est la plus proche de la réalité.

3.3 / Méthodes d'analyse de sûreté de fonctionnement

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

- des défaillances et des pannes des composants du système,
- des évènements liées 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/APR Analyse Préliminaire des Dangers,(Risques)
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.

Nous ne verrons dans la suite que quelques-unes de ces méthodes.