LA SÛRETÉ DE FONCTIONNEMENT

Le but de la sûreté de fonctionnement (dependability, SdF) est d’évaluer les risques potentiels, prévoir l’occurrence des défaillances et tenter de minimiser les conséquences des situations catastrophiques lorsqu’elles se présentent.

Définition de Laprie 89 : la sûreté de fonctionnement d’un système informatique est la propriété qui permet de placer une confiance justifiée dans le service qu’il délivre.

Définition CEI 50(191) : Aptitude d’une entité à assumer une ou plusieurs fonctions requises dans des conditions données.

* **Identifier** les défaillances de la manière la plus exhaustive possible.
* **Prioriser** l’importance des risques qu’elles impliquent.
* D’un point de vue système il faudra **prévoir l**es défaillances.
* Au cours de la vie du système il faudra savoir **mesurer** les défaillances et capitaliser ces observations.
* Le but final étant bien sûr de **maîtriser** ces défaillances.

La SdF est ainsi qualifiée parfois de « sciences des défaillances ».

**Les défaillances**

 Définition CEI 50(191) :

* La défaillance est la cessation de l’aptitude d’une entité à accomplir une fonction requise.
* La défaillance est un événement, elles est donc présente ou non et peut se combiner avec un ou plusieurs **événements.**
* La définition précédente implique la connaissance de la fonction requise et la définition de sa cessation
* Plusieurs classifications des défaillances sont alors possibles.

 **Classification des défaillances**

****

****

**Classification des défaillances**

* Par les effets :
* **Défaillance mineure** : nuit au bon fonctionnement en causant un dommage négligeable au système ou à son environnement. Pas de risque humain.
* **Défaillance significative** : nuit au bon fonctionnement sans dommage notable. Pas de risque humain important.notable. Pas de risque humain important.
* **Défaillance critique** : perte de ou des fonctions essentielles du système. Dégâts important au système ou son environnement. Pas de risque motel ou de blessure pour l’homme.
* **Défaillance catastrophique** : perte de ou des fonctions essentielles du système. Dégâts important au système ou son environnement. Risque mortel ou de blessures graves pour l’homme.
* Par les causes :
* **défaillance primaire** (ou première) d’une entité: dont la cause directe ou indirecte n'est pas la défaillance d'une autre entité.
* **défaillance secondaire** (ou seconde) d’une entité : dont la cause directe ou indirecte est la défaillance d'une autre entité. L'entité devenant alors indisponible (nécessité de réparation) après disparition devenant alors indisponible (nécessité de réparation) après disparition de la cause.
* **défaillance par (de) commande** d’une entité: dont la cause directe ou indirecte est la défaillance d'une autre entité, mais elle redevient disponible après disparition de la cause.

Ceci implique que l’on recherchera la cause de la défaillance

**De la faute à la défaillance**

* **Faute** : cause interne de la défaillance
* **Erreur** : manifestation interne (signal/état incorrect)
* **Défaillance** : service rendu incorrect
* **Conséquence** : manifestation externe



La faute peut être introduite par le concepteur, l’utilisateur ou l’environnement. Elle rend l’entité imparfaite.

**Classification des fautes**

On peut donner quelques critères de classification des fautes :

* Accidentelle -Intentionnelle
* Physique - Humaine
* Interne - Externe
* Active (qui produit une erreur) - Dormante
* Douce - Dure
* Permanente - Temporaire / Transitoire
* Opérationnelle - De conception

**Les composantes de la SdF**



**La Fiabilité**

* Définition CEI 50(191) : la fiabilité est l’aptitude d’une entité à accomplir une fonction requise, dans des conditions données, pendant un **intervalle de temps** donné.

 **Mesure** : La fiabilité se mesure par la **probabilité** qu'une entité a ccomplisse une fonction requise dans les conditions données pendant l'intervalle de temps [o,t].

**Evaluation(s)** : opérationnelle (observée), extrapolée, prévisionnelle (conception + fiab. Composant), intrinsèque (programme d’essai).

Considérons l’instant **T** d’occurrence de la défaillance ; cette variable aléatoire permet de définir la notion de fiabilité qui s’interprète comme la probabilité que l’entité considérée ne tombe pas en panne avant un instant t donné ou bien comme la probabilité qu’elle tombe en panne après l’instant t.

On peut noter : R ( t ) = P (E non défaillante sur la durée [0, t], en supposant qu’elle n’est pas défaillante à l’instant t = 0).

Ce qui peut s’exprimer par : **R ( t ) = P ( T > t )**

L’aptitude contraire est appelée défiabilité, et est définie par :

**F(t)= 1 - R (t ) = P( t> T) = F( t)**