

Introduction

Qu'est-ce que la sureté de fonctionnement

La sureté 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.

Définition 1 (SdF) : La sureté 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.

Définition 2 (Laprie96) : La sureté de fonctionnement d'un système informatique est la propriété qui permet de placer une confiance justifiée dans le service qu'il délivre.

Il existe de nombreuses définitions, de standards (qui peuvent varier selon les domaines d'application nucléaire, spatial, avionique, automobile, rail . . .).

On peut néanmoins considérer que le Technical Committee 56 Dependability de l'International Electrotechnical Commission (IEC) développe et maintient des standards internationaux reconnus dans le domaine de la sureté 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.

La SdF utilise des techniques qualitatives et quantitatives qui font appel aux domaines des statistiques et des probabilités.

Pour modéliser puis quantifier le comportement des équipements par la sûreté de fonctionnement, il est nécessaire au préalable de définir des paramètres représentatifs et de les observer.

Les paramètres décrivant un équipement sont :

- les durées de fonctionnement avant défaillance,
- les durées de réparation.

Ces durées sont aléatoires, et il est nécessaire de les combiner pour quantifier le comportement de l'équipement.

Fiabilité d'une entité E (notée $R(t)$)

$R(t)$ = Probabilité que E soit non défaillante sur $[0, t[$

Défiabilité $(t) = 1 - R(t)$

Disponibilité d'une entité E (notée $A(t)$)

$A(t)$ = Probabilité que E soit non défaillante à l'instant t

Indisponibilité $(t) = 1 - A(t)$

Maintenabilité d'une entité (notée $M(t)$)

$M(t)$ = Probabilité que E soit réparée sur $[0, t[$