Cours :
Sûreté de Fonctionnement

Description de la matière

Objectifs:

- Maîtriser les outils et les méthodes industriels de la Sûreté de Fonctionnement utilisés dans l'industrie pour gérer un projet et en assurer sa qualité.
- Mettre en place les connaissances, les réflexes et les attitudes pour la prise en compte des activités Sûreté de Fonctionnement au niveau adéquat pour un projet industriel.

But de la sûreté de fonctionnement

- Le but de la sûreté de fonctionnement : mesurer la qualité de service délivré par un système, de manière à ce que l'utilisateur ait en lui une confiance justifiée.

- Cette confiance justifiée s'obtient à travers une analyse qualitative et quantitative des différentes propriétés du service délivré par le système, mesurée par les grandeurs probabilistes associées : fiabilité, maintenabilité, disponibilité, sécurité.

Chapitre 1:

Sûreté de Fonctionnement:

Notions de base

Plan :

1. Introduction
2. Concepts
3. Définitions
4. Moyens de la SdF
5. Entraves de la SdF
6. Composantes de la SdF

1. Introduction

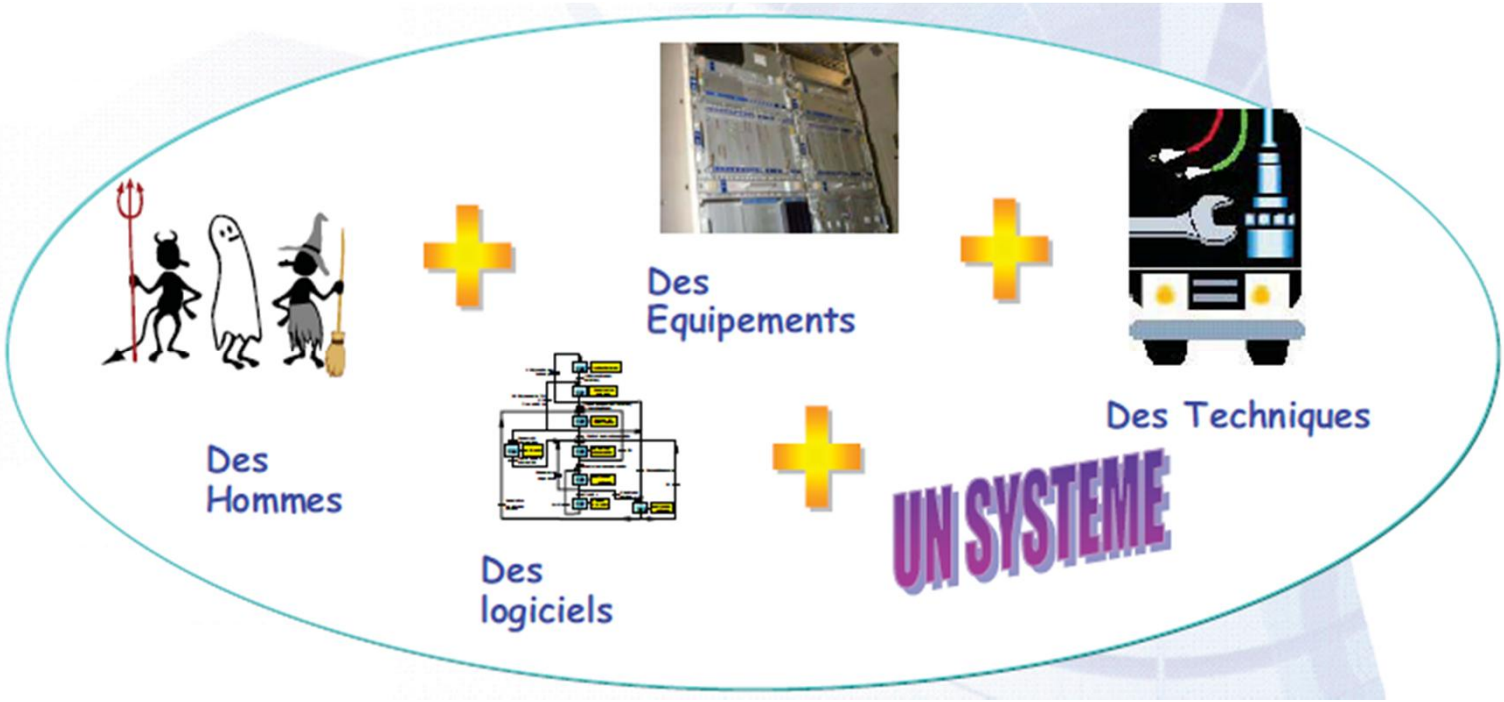
1. Introduction

La sûreté de fonctionnement est apparue comme une nécessité au cours du XX^{ème}, notamment avec la révolution industrielle. Le terme *dependability* est apparu dans une publicité sur des moteurs Dodge Brothers dans les années 1930. L'objectif de la sûreté de fonctionnement est d'atteindre le Graal de la conception de système : zéro accident, zéro arrêt, zéro défaut (et même zéro maintenance). Pour pouvoir y arriver, il faudrait tester toutes les utilisations possibles d'un produit pendant une grande période ce qui est impensable dans le contexte industriel voire même impossible à réaliser tout court. La sûreté de fonctionnement est un domaine d'activité qui propose des moyens pour augmenter la fiabilité et la sûreté des systèmes dans des délais et avec des coûts raisonnables.

Introduction

Qu’est ce qu’un système ?

Qu’est ce qu’un système ?



Ensemble complexe de matériels, logiciels, personnels et processus d’utilisation, organisés de manière à satisfaire les besoins et à remplir les services attendus, dans un environnement donné.

L'objet sous étude est le système et les fonctions qu'il fournit. Il existe de nombreuses définitions de système dans le domaine des systèmes d'ingénierie.

Définition 3 (Un système) *Un système peut être décrit comme un ensemble d'éléments en interaction entre eux et avec l'environnement dont le comportement dépend :*

- *des comportements individuels des éléments qui le composent,*
- *des règles d'interaction entre éléments (interfaces, algorithmes, protocoles),*
- *de l'organisation topologique des éléments (architectures).*

Le fait que les sous-systèmes sont en interaction implique que le système n'est pas simplement la somme de ses composants. En toute rigueur, un système dans lequel un élément est défaillant devient un nouveau système, différent du système initial.

Exemple 1 *Une installation chimique, une centrale nucléaire ou un avion sont des systèmes. Le contrôle-commande est un sous-système, une vanne ou un relais sont des composants. La nature technologique d'un système est variée : électrique, thermo-hydraulique, mécanique ou informatique.*

Assurer les fonctions Tout système se définit par une ou plusieurs fonctions (ou missions) qu'il doit accomplir dans des conditions et dans un environnement donnés. L'objet d'étude de la sûreté de fonctionnement est la *fonction*. Une fonction peut être définie comme l'action d'une entité ou de l'un de ses composants exprimée en terme de finalité. Il convient de distinguer les fonctions et la structure (ou encore architecture matérielle support).

- fonction principale : raison d'être d'un système (pour un téléphone portable, la fonction principale est la communication entre 2 entités) ;
- fonctions secondaires : fonctions assurées en plus de la fonction principale (sms, horloge, réveil, jeux . . .) ;
- fonctions de protection : moyens pour assurer la sécurité des biens, des personnes et environnement ;
- fonctions redondantes : plusieurs composants assurent la même fonction.

Une description fonctionnelle peut généralement se faire soit par niveau soit pour un niveau donné. Une description par niveau est une arborescence hiérarchisée. On donne l'exemple d'une description fonctionnelle d'une machine à laver dans la figure 3.

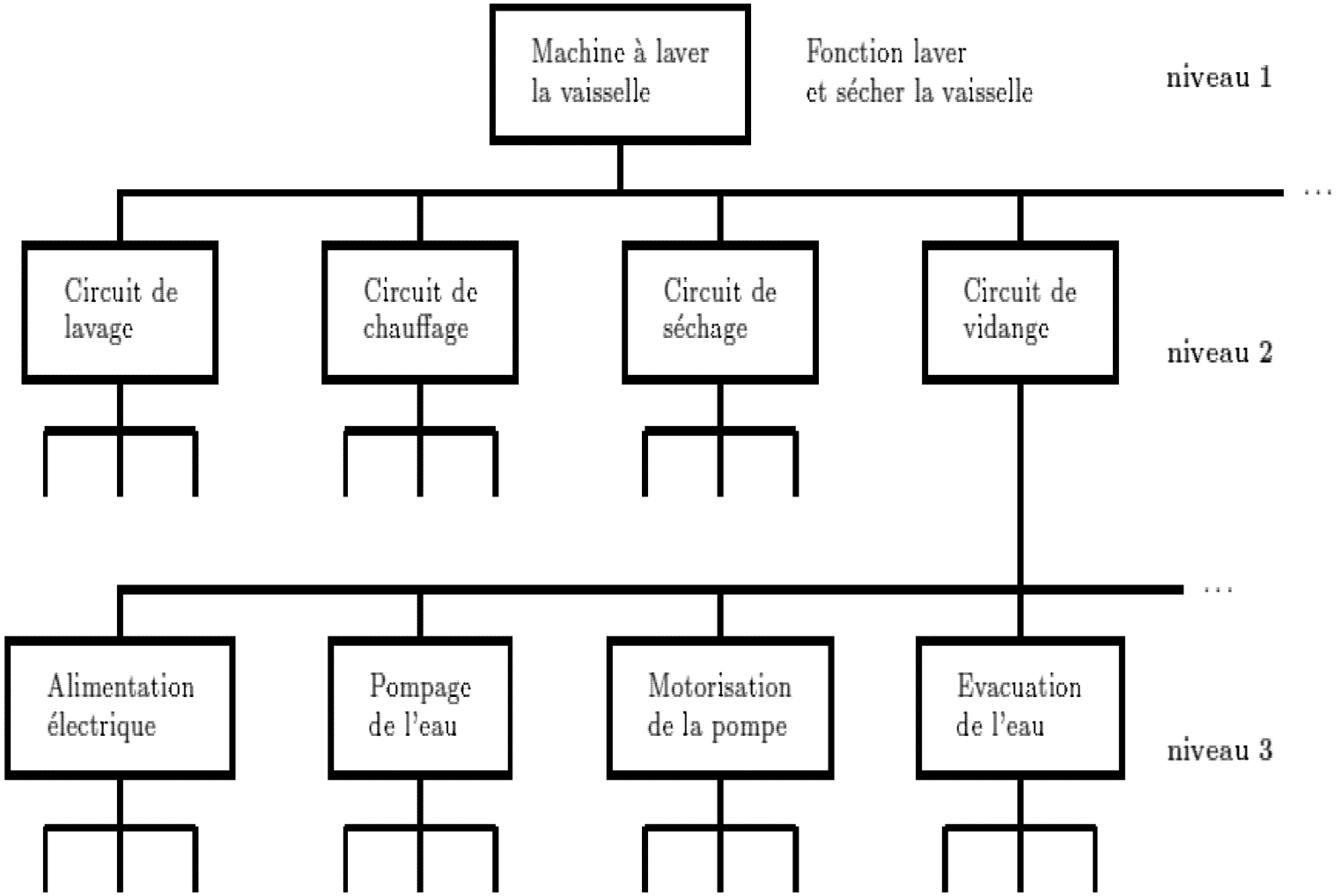


FIGURE 3 – Description fonctionnelle d'une machine à laver la vaisselle

2.Concepts…

HISTORIQUE

Jusqu'à la Renaissance et au-delà, on a toujours pensé que la fiabilité d'une chaîne reposait sur celle de son maillon le plus faible. Ainsi, si R était la fonction de fiabilité (ou de survie), alors en fonction du temps, on pensait pouvoir écrire : $R_{chaîne}(t) = Min1 \leq i \leq n * R_i(t)$, où les items indexent les n maillons de la chaîne. Or, il s'est avéré que, dans une chaîne, ce n'était pas systématiquement le maillon le plus faible qui se rompait en premier. La fiabilité de la chaîne est alors devenue une certaine fonction de la fiabilité de ses maillons, les plus faibles participant davantage que les plus solides à l'éventualité d'une rupture.

- **L'époque moderne**

Par la suite, des problèmes de fiabilité se sont posés lors de la conquête de l'Ouest. Les composants mécaniques les plus critiques de l'époque étaient les roulements à billes des locomotives à vapeur ! De même, les freins de ces mêmes locomotives, en service entre 1861 et 1883, seront abandonnés pour des problèmes de fiabilité, notamment sur les connexions électriques entre les wagons, et les premiers freins pneumatiques les remplaceront.

Ceux-ci sont toujours d'actualité. La houille blanche, cette nouvelle énergie électrique, va constituer une formidable source de puissance qu'il va rapidement falloir apprendre à domestiquer et à fiabiliser.

Les premiers appareils construits dans cette optique (transformateurs, lignes de tension, interconnexions de lignes) vont permettre de diffuser l'énergie grâce à la mise en redondance et à l'amélioration des matériels, mais engendreront des problèmes de sûreté dramatiques.

C'est l'absence préalable d'étude de sûreté approfondie qui coûtera au métro parisien ses 84 morts en 1903, puis au Titanic son naufrage en 1912.

Durant la 1ère Guerre Mondiale, les bateaux construitrapidement pour amener les soldats américains sur le sol européen ne résisteront que très difficilement aux eaux gelées de l'Atlantique Nord, subissant beaucoup de fissures dans les coques et de multiples naufrages.

- **Les années 1930**

Dès 1930, les transports aériens commencent à collecter des informations statistiques sur les moteurs et les accidents des appareils. Les premiers objectifs quantifiés sont promus par le capitaine A.F.Pugsley de la 7ème brigade d'infanterie canadienne, entre 1939 et 1942, avec un taux de défaillance évalué à 10-5/h pour les avions, dont 10-7/h pour leur structure.

- **Les années 1940**

Les années 1940 voient le formidable essor des techniques de fiabilité. En Allemagne, W. Von Braun met au point ses V1 et revient sur l'idée que la fiabilité d'une chaîne est celle de son maillon le plus faible, en essayant de prouver que la fiabilité d'une chaîne est la moyenne de la fiabilité de ses constituants. Les essais montreront que cette hypothèse était également erronée. C'est Eric Pieruschka qui va finalement donner la formule de calcul de la fiabilité d'une chaîne : Rchaîne(t)= $P_i \leq i \leq nR_i(t)$. La probabilité de survie d'une chaîne à une date t arbitraire est le produit des probabilités de survie de chacun de ses composants à cette date, dans l'hypothèse où lesdits composants sont indépendants les uns des autres. Aux Etats-Unis, pendant ce temps, les nouvelles techniques permettent de gagner un facteur 4 sur la durée de vie des moteurs de traction des locomotives, pour dépasser le million de miles.

- **Les années 1950**

On assiste à l'avènement du concept de maintenance : $1 en équipement génère $2 en maintenance. C'est à cette époque que la marine militaire américaine prend conscience que ses tubes électroniques ne sont opérationnels qu'à hauteur de 30 % de leur temps d'utilisation.

Les premières directives en électronique voient le jour, avec des spécifications d'essais de vieillissement accéléré, directives qui seront reprises et adaptées par la NASA. Les toutes nouvelles centrales nucléaires entraînent les premières études sur la fiabilité humaine.

En France, c'est le Centre national d'Etudes sur les Télécommunications qui commence ses travaux sur un recueil de données de fiabilité électronique.

- **Les années 1960**

Les industries aéronautiques et spatiales (Mac-Donnell Douglas) effectuent les premières analyses relatives aux défaillances de composants, pour accompagner les débuts du programme Apollo.

Dans le nucléaire, on assiste aux premiers pas de la méthode du Diagramme de Succès. L'armée américaine (DoD : Department of Defence) promulgue les premières vraies exigences de sûreté de fonctionnement suite à des accidents sur des missiles. Aux Bell Labs, en 1961, le nouveau concept d'arbre des causes est utilisé avec succès sur le projet de missile Minuteman ; cette technique sera reprise par Boeing. En France, la SNIAS (Société nationale des Industries aéronautiques et spatiales) utilise la méthode des combinaisons de pannes sur le projet Concorde, puis sur Airbus. Toutes ces méthodes trouvent un écho favorable dans l'industrie civile, notamment au Japon ; apparaissent alors les premières bases de données et les premiers ouvrages de référence.

Dans un souci d'harmonisation et de standardisation, la Commission électrotechnique internationale crée le Comité technique 56 "Dependability" en octobre 1965 ; les produits de ce groupe deviendront des normes internationales en 1976. L'Académie des Sciences accueille le mot "fiabilité" dans sa terminologie en 1962. En 1965 est introduit le concept de maintenabilité sur lequel le CEA travaillera activement dans les années 67-68.

- **Les années 1970-80**

En 1971 sont publiés les résultats des premiers travaux sur la fiabilité du logiciel. En 1972, EDF et le CEA mènent les premières études exhaustives sur le nucléaire. En 1975, le rapport américain Rasmussen présente une évaluation complète d'un risque nucléaire sur les centrales de Surry 1 et Peach Bottom 2 : en synthèse, le risque calculé pour les populations avoisinant lesdites centrales est inférieur à celui que font courir les chutes de météorites. En 1979, c'est la catastrophe nucléaire de TMI (Three Miles Island) ; une manière inattendue de promouvoir les outils de sûreté de fonctionnement, puisque le scénario qui a mené à la catastrophe était quasiment décrit dans le rapport Rasmussen ! Puis ce sont les industries pétrochimiques qui procèdent à leurs premières études de risque, avant que les techniques de sûreté de fonctionnement ne soient diffusées dans la chimie, le ferroviaire, l'automobile, le traitement et l'épuration d'eau, et l'ensemble des grands secteurs industriels.

- **Aujourd'hui**

La réglementation, et les certifications qu'elle impose, a eu un double effet : le développement de l'utilisation des outils de sûreté de fonctionnement, mais également une certaine idée de la couverture des risques.

N'a-t-on pas oublié que, malgré les études, les précautions, les systèmes de sauvegarde, les protections, le risque existe toujours ?

Dans les procès qui font suite aujourd'hui à la plupart des accidents, il semble que la notion de risque ait été peu à peu effacée pour laisser place à celle de tort ou responsabilité. Comme si tous les risques de notre vie courante pouvaient être prévus et annihilés.

En parallèle, la compétition continue que se livrent les grands groupes les force à disposer d'une productivité la meilleure possible, et donc à réduire les arrêts de production et à maximiser la disponibilité de leurs équipements.

Enfin, la sécurité des biens et des personnes n'a jamais semblé aussi importante qu'aujourd'hui aux yeux de nos concitoyens. En témoignent les actions vigoureuses autour de la notion de malveillance (intrusion par effraction, attaque, vol, piratage).

Dans les deux cas, la pression médiatique et écologique autour des accidents notables (plate-forme Piper Alpha, accident chimique de Bophal et d'AZF, ou catastrophe aérienne de la TWA) est telle qu'elle entraine des conséquences très lourdes pour l'entreprise.

1.1.2 Coût de la sûreté de fonctionnement

Le coût d'un haut niveau de sûreté de fonctionnement est très onéreux. Le concepteur doit faire des compromis entre les mécanismes de sûreté de fonctionnement nécessaires et les coûts économiques. Les systèmes qui ne sont pas sûrs, pas fiables ou pas sécurisés peuvent être rejetés par les utilisateurs. Le coût d'une défaillance peut être extrêmement élevé. Le coût de systèmes avec un faible niveau de sûreté de fonctionnement est illustré dans les figures ci-dessous.

Coût moyen d'indisponibilité

Secteur industriel	Production et distribution d'énergie	2,8	Millions d'Euros par heure perdue
	Production manufacturière	1,6	
	Institutions financières	1,4	
	Assurances	1,2	
	Commerce	1,1	
	Banques	1	

Quelques chiffres

Coût annuel des défaillances informatiques

Estimation compagnies d'assurance (2002)	France (secteur privé)	USA	Royaume Uni
Fautes accidentelles	1,1 G€	4 G$	
Malveillances	1,3 G€		1,25 G£
Estimation globale	USA : 80 G$	EU : 60 G€	

Quelques chiffres

Coûts de maintenance

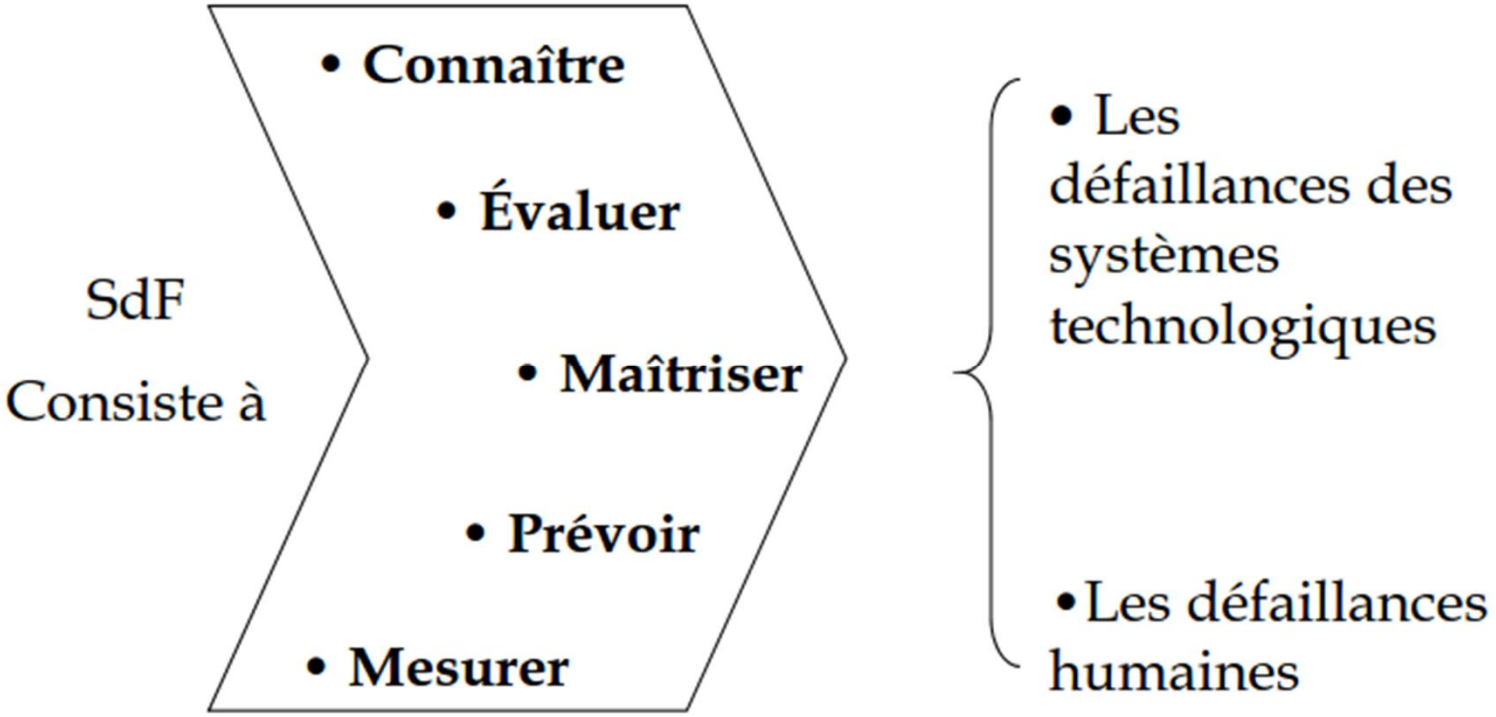
Logiciel embarqué de la navette spatiale : 100 M $ / an

Coût logiciels abandonnés (défaillance du processus de développement)

	Succès	Remise en question	Abandon
USA [Standish Group, 2002, 13522 projets]	34%	51%	15%

~ 38 G$ de pertes (sur total 225 G$)

Les enjeux de la sûreté de fonctionnement



Domaines d’application

- Ensemble des domaines industriels
- Études prévisionnelles
- Études opérationnelles

- Différentes méthodes pour différentes applications

3.Définitions

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 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 sûreté 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 sûreté 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 sûreté 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.

Entité

La fonction d’un système :

C’est ce à quoi le système est destiné, elle inclut les performances attendues du système.

Le comportement d'un système :

c'est ce que le système fait pour accomplir sa fonction,

et il est décrit par une séquence d'états.

Le service délivré par un système :

son comportement tel que perçu par son ou ses utilisateurs.

Un utilisateur :

est un autre système, éventuellement humain, qui est en interaction avec le système considéré

l’interface du service :

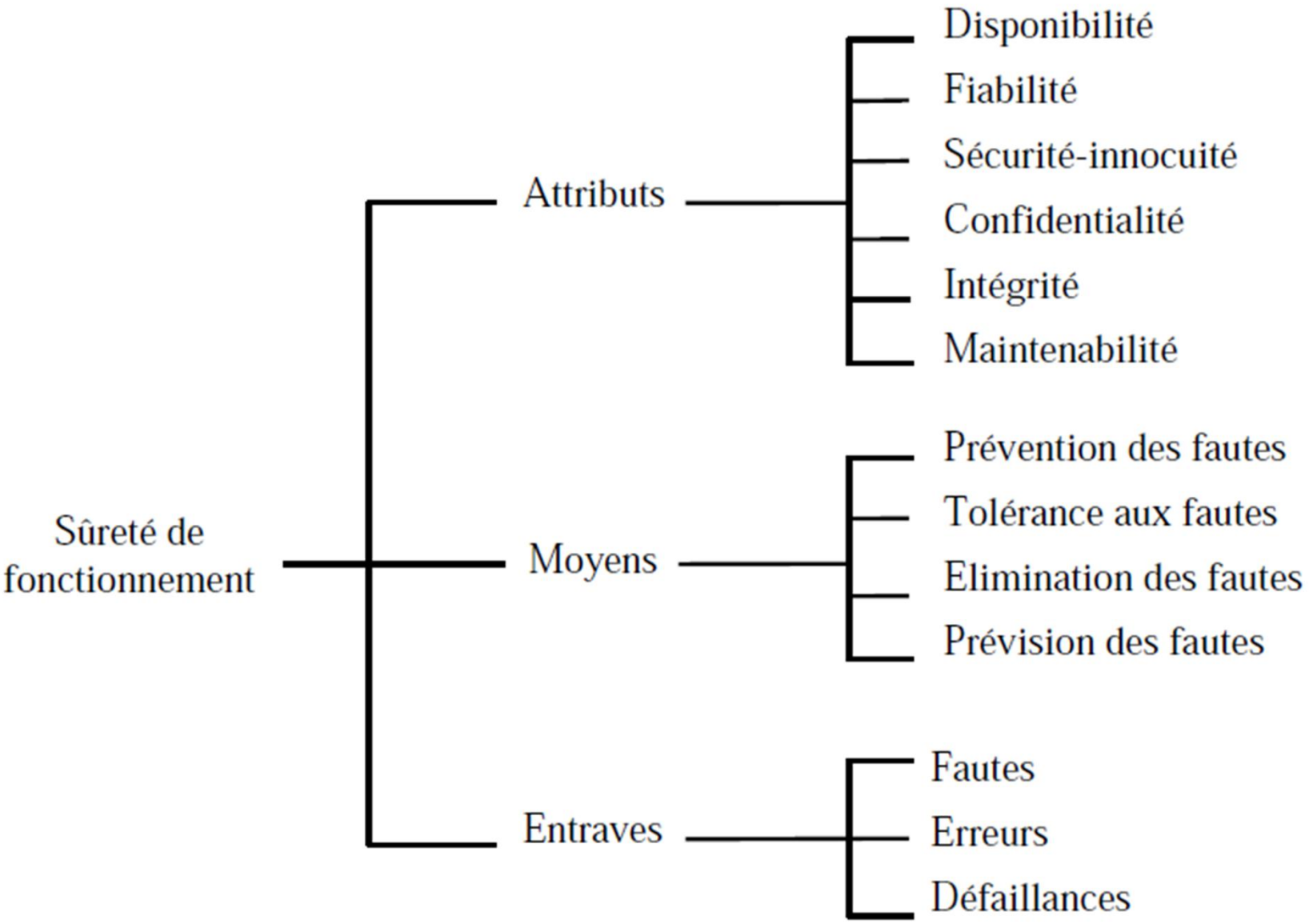
La partie de la frontière du système où ont lieu les interactions avec ses utilisateurs

Un service est considéré correct si et seulement si le service délivré accomplit la fonction du système.

La défaillance:

un événement qui survient lorsque le service délivré dévie du service correct, soit parce qu'il n'est plus conforme à la spécification, soit parce que la spécification ne décrit pas de manière adéquate la fonction du système.

La sûreté de fonctionnement peut aussi être définie comme l'aptitude à éviter des défaillances du service plus fréquentes ou plus graves que ce qui est acceptable.


Sûreté de fonctionnement
Attributs
Disponibilité
Fiabilité
Sécurité-innocuité
Confidentialité
Intégrité
Maintenabilité
Moyens
Prévention des fautes
Tolérance aux fautes
Elimination des fautes
Prévision des fautes
Entraves
Fautes
Erreurs
Défaillances

4. Composantes de la SdF

4. Composantes de la SdF

la SdF est définie par un certain nombre de composantes (FMDS) :

1. Fiabilité
2. Maintenabilité
3. Disponibilité
4. Sécurité

Fiabilité :

Aptitude d'un système à accomplir sa mission dans des conditions données.

Exemples :

- Ma voiture me permettra d'accomplir le trajet prévu dans les conditions prévues, compte tenu des conditions de circulation (elle n'aura pas de panne durant le trajet).
- La machine ne doit pas interrompre la production par ses défaillances.

Maintenabilité :
Aptitude d'un système à être maintenu ou à reprendre l'accomplissement de sa fonction après défaillance.

Exemple :

Lorsque la voiture est chez le garagiste (pour entretien programmé ou réparation), la durée d'immobilisation et le coût doivent être les plus faibles possibles.

Disponibilité :
Aptitude d'un système à fonctionner quand on en a besoin.

Exemple :

- Ma voiture est "prête" lorsque je veux l'utiliser (elle n'est pas chez le garagiste, elle est en état de marche).

Sécurité :

Propriété d'un système de présenter, pour son environnement et pour lui même, un risque, déterminé en fonction des dangers potentiels inhérents à sa réalisation et à sa mise en œuvre, qui ne soit pas supérieur à un risque convenu.

5. Moyens de la SdF

5. Moyens de la SdF

Prévention des fautes:

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.

Tolérance aux fautes:

Consiste à mettre en place des mécanismes qui maintiennent le service fourni par le système, même en présence de fautes.

Elimination des fautes:

- Pendant la phase de développement, l'idée est d'utiliser des techniques de vérification avancées de façon à 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.

Prévision des fautes:

consiste à anticiper les fautes (de manière qualitative ou probabiliste) et leur impact sur le système.

6. Entraves à la SdF

Les entraves à la sûreté de fonctionnement représentent les circonstances indésirables, mais non inattendues, causes ou résultats de la non sûreté de fonctionnement ; la confiance ne peut plus, ou ne pourra plus, être placée dans le service délivré.

1.3.1 La défaillance

C'est la cessation de l'aptitude d'une entité à accomplir une fonction requise. On dira qu'une entité connaît une défaillance lorsqu'elle n'est plus en mesure de remplir sa (ou ses) fonctions. (A. Villemeur).

Evénement survenant lorsque le service délivré dévie de l'accomplissement de la fonction du système. (J.C. Laprie)

Une entité connaît une défaillance lorsqu'elle n'est plus en mesure de remplir sa (ou ses) fonction(s). Par extension, on considère parfois qu'il y a une défaillance lorsqu'il y a altération de l'aptitude d'une entité à accomplir une fonction requise : les tolérances associées doivent alors être définies. Afin de préciser cette notion de défaillance, on réalise plusieurs classifications des défaillances.

1.3.2 Classification des défaillances

1.3.2.1 En fonction de la rapidité de leur manifestation

Défaillance progressive : elle se manifeste par une évolution progressive des caractéristiques d'une entité.

Défaillance soudaine : elle se manifeste par une perte soudaine des caractéristiques d'une entité.

1.3.2.2 En fonction de leur amplitude

Défaillance partielle : défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, mais telle qu'elle n'entraîne pas une disparition complète de la fonction requise (Commission Electrotechnique Internationale : CEI).

Défaillance complète : défaillance résultant de déviation d'une ou des caractéristiques au-delà des limites spécifiées, telle qu'elle entraîne une disparition complète de la fonction requise (CEI).

1.3.2.3 En fonction de la rapidité et de l'amplitude

Défaillance catalectique : défaillance qui est à la fois soudaine et complète (CEI).

Défaillance par dégradation : défaillance qui est à la fois progressive et partielle (CEI).

1.3.2.4 En fonction des causes

Défaillance première : défaillance d'une entité dont la cause directe ou indirecte n'est pas la défaillance d'une autre entité (A. Villemeur).

Défaillance seconde : défaillance d'une entité dont la cause directe ou indirecte est la défaillance d'une autre entité et pour laquelle cette entité n'a pas été qualifiée et dimensionnée (A. Villemeur).

Défaillance de commande : défaillance d'une entité dont la cause directe ou indirecte est la défaillance d'une autre entité et pour laquelle cette entité a été qualifiée et dimensionnée (A. Villemeur).

1.3.2.5 En fonction des effets

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

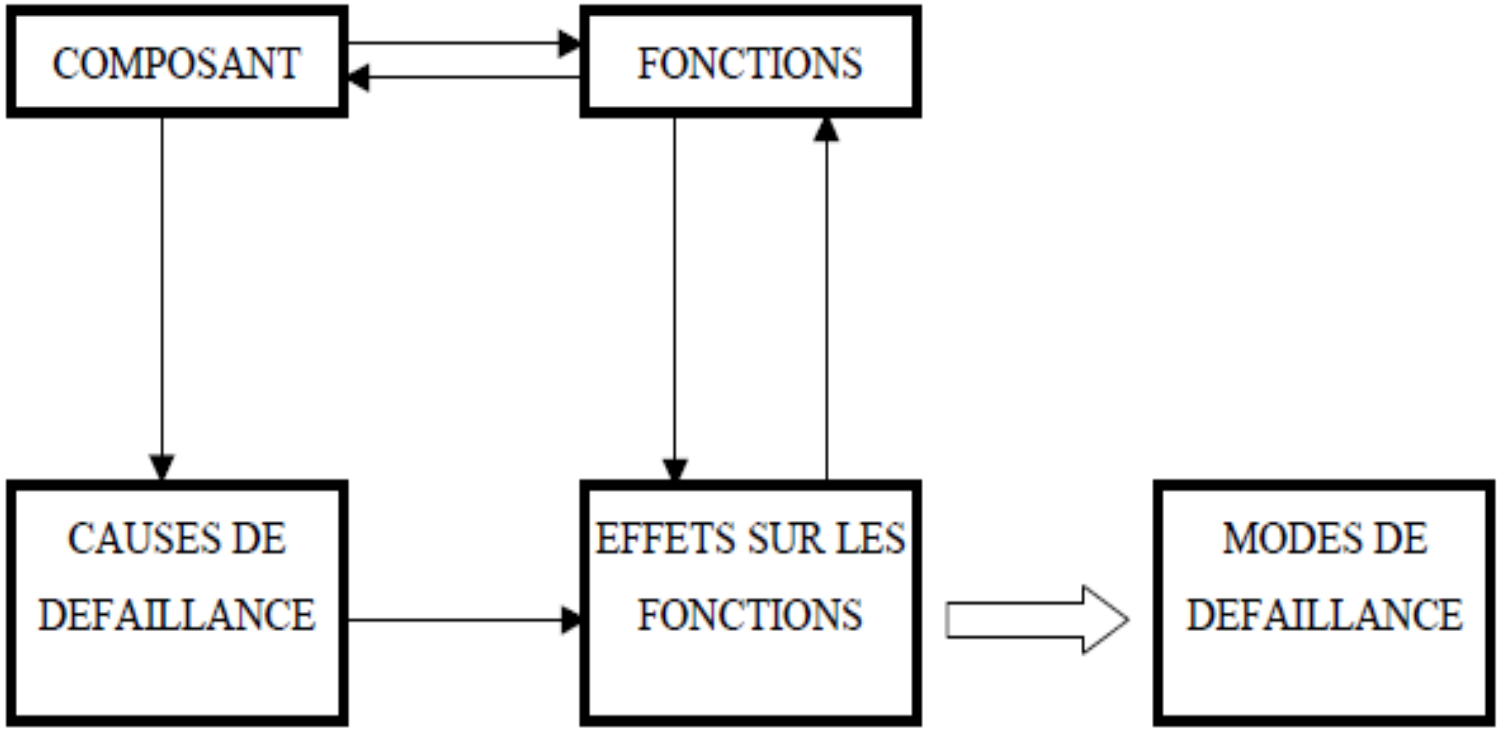
Défaillance significative : défaillance qui nuit au bon fonctionnement d'un système sans toutefois causer de dommage notable, ni présenter de risque important pour l'homme (C. Lievens).

Défaillance critique : défaillance qui entraîne la perte d'une (ou des) fonction(s) essentielles d'un système et cause des dommages importants au dit système ou à son environnement en ne présentant, toutefois, qu'un risque négligeable de mort ou de blessure. (C. Lievens).

Défaillance catastrophique : défaillance qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) d'un système en causant des dommages importants au dit système ou à son environnement et/ou entraîne, pour l'homme, la mort ou des dommages corporels (C. Lievens).

1.3.3 Les modes de défaillance

Un mode de défaillance est l'effet par lequel une défaillance est observée (CEI).



1.3.4 Un modèle phénoménologique

le triplet < défaut, panne, erreur >

Le défaut

Le défaut est un phénomène adverse qui a une origine physique ou humaine.
Le défaut physique peut être d'origine interne (désordre physico-chimique, dégradation) ou externe (perturbation de l'environnement) au système considéré.
Le défaut humain peut être d'origine conceptuelle ou d'interaction. Les défauts de conception sont des défauts de développement accidentels ou intentionnels, sans volonté de nuire. Les défauts d'interaction sont d'origine externe au système, accidentel ou intentionnel sans volonté de nuire.

La panne

La panne est l'effet fonctionnel local du défaut et elle existe dès que le défaut apparaît. Elle peut être dormante ou active. Si une panne devient active alors elle produit une erreur.

1.3.4 Un modèle phénoménologique

L'erreur

L'erreur est l'effet fonctionnel global du défaut ; c'est la partie de l'état du système qui est susceptible d'entraîner une défaillance.
Une erreur peut être latente ou détectée : elle est latente tant qu'elle n'a pas été détectée. Si l'erreur affecte le service délivré, alors on dit qu'il y a une défaillance.