# SURETE DE FONCTIONNEMENT

## Historique

La sureté de fonctionnement **SdF** est apparue comme une nécessité au cours du XX$^{ème}$ avec la révolution industrielle. Le tableau 1 présente son historique.

**Tableau 1-** *Historique de la sureté de fonctionnement.*

| Périodes | Concepts | Evénements |
|---|---|---|
| Année 1950 | Approche statistique, taux de défaillance.<br>Théorie de la fiabilité en électronique (USA) | Explosion poudrière (1794)<br>Accident chemin de fer(1842)<br>Titanic (1912). |
| Année 1960 | Quantification de la disponibilité<br>Arbres des causes(NASA)<br>Analyse des défaillances et leurs effets en (aéronautique et le spatial). | |
| Année 1970 | Analyse des risques (Nucléaire)<br>Collecte de données | |
| Année 1980 | Formalisation et généralisation de la SdF (conception des systèmes complèxe)<br>Nouvelles techniques simulation Modélisation | Tchernobyl (1986)<br>Ariane V (1996) |
| 2000 | Utilisation de la SdF dans l'industrie | |

## Objectif

L'objectif de la **SdF** est d'atteindre la conception des différents systèmes avec: **zéro accident, zéro arrêt, zéro défaut et zéro maintenance**. Pour Pouvoir y arriver, il faudrait tester toutes les utilisations d'un produit pendant une grande période. La **SdF** est un domaine d'activité qui propose des moyens pour augmenter la fiabilité et la sureté des systèmes dans les délais et avec des couts raisonnables.

## Définition

La **SdF** consiste à : - Évaluer les risques potentiels ;
- Prévoir les défaillances ;

- Minimiser les conséquences des catastrophes lorsqu'elles se présentent.

La **Sdf** d'un système est la propriété qui permet de placer une *confiance justifiée* dans le service qu'il délivre. Elle est aussi l'aptitude d'un système à *satisfaire* une ou plusieurs fonctions requises dans des conditions données.

Elle est définie comme la *science des défaillances* qui inclut leur :

- Connaissance ;
- Evaluation ;
- Prévision ;
- Maitrise.

Différents concepts peuvent être définis comme suit :

***Symptôme*** : Observation de dérive ;

***Erreur* / Defect :** La cause de la défaillance est une erreur affectant une Partie de l'état du système susceptible d'entraîner la défaillance

*Erreur affectant le service → indication d'occurrence d'une défaillance*

***Défaillance* / Failure** :

**Tableau 2-** *Classification des défaillances en fonction des effets*

| Classes | Effets |
|---|---|
| **Défaillance mineure** (minor) | Défaillance qui nuit au bon fonctionnement d'un système en Causant un dommage négligeable au système ou à son environnement sans présenter de risque pour l'homme. |
| **Défaillance significative** (major) | Défaillance qui nuit au bon fonctionnement sans causer de dommage notable ni présenter de Risque important pour l'homme. |
| **Défaillance critique** (hazardous) | Défaillance entrainant la perte de fonction(s) essentielle(s) et cause des dommages importants au système en ne présentant qu'un risque négligeable de mort ou de blessure. |
| **Défaillance catastrophique** (catstrophic) | Défaillance occasionnant la perte de fonction(s) essentielle(s). En causant des dommages importants au système ou a son environnement et/ou entraine la mort ou des dommages corporels. |

Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise. Elles peuvent avoir des effets différents dans un système . Certaines défaillances

n'affectent pas directement les fonctions du système et ne nécessitent qu'une action corrective. D'autres, affectent la disponibilité ou la sécurité.

La défaillance d'une entité résulte de causes de défaillance. Ces causes sont le résultat d'activation d'erreur suite à des fautes. On utilise généralement, une échelle de gravité des effets et on considère traditionnellement deux catégories de défaillances représentées dans le tableau 2.

## 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 d'une entité en panne pour une fonction donnée. On classe les modes de défaillance en quatre catégories représentées par le Tableau 3.

**Tableau 3** – *Classification des modes de défaillance*

| Mode de défaillance | Explication |
|---|---|
| Fonctionnement prématuré (ou intempestif) | Fonctionne alors que ce n'est pas prév à cet instant |
| Ne fonctionne pas au moment pré | Ne démarre pas lors de la sollicitation |
| Ne s'arrête pas au moment prévu | Continue son service qui n'est pas prév |
| Défaillance en fonctionnement | |

**Taux de défaillance / Failure rate :**

Il est fréquent que les entités présentent des taux de défaillance en fonction du temps suivant une courbe dite en baignoire, voire figure 1.

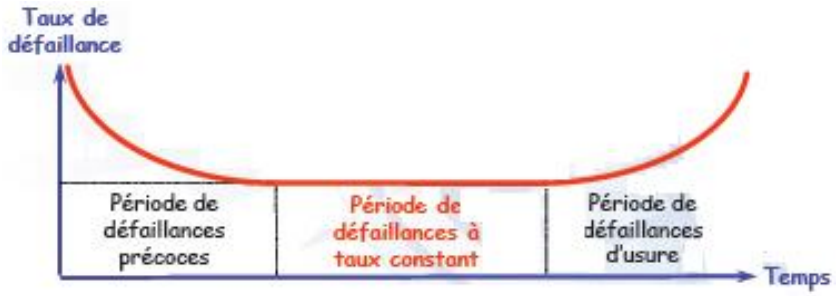


**Figure 1** – *Taux de défaillance en fonction du temps*

**Faute / Fault :** La cause de l'erreur est une faute (un court-circuit, une perturbation électromagnétique ou une faute de développement logiciel). Cause adjugée ou supposée d'une erreur.

**Panne :** La panne est l'inaptitude d'une entité à accomplir une mission. Une panne résulte toujours d'une défaillance. Les relations entre les notions précédentes sont décrites dans la figure 2. La défaillance d'un composant est une faute pour le système qui le contient. Ainsi, les défaillances résultent souvent de phénomènes de propagations d'erreur.

On peut conclure que la **SdF** est la science des défaillances, elle inclut leur connaissance, leur évaluation, leur prévention, leur mesure et leur maitrise. Il s'agit d'un domaine qui nécessite une connaissance du système comme les conditions d'utilisation, les risques extérieurs, les architectures fonctionnelle, la structure et fatigue des métaux, ainsi les rapports des accidents.

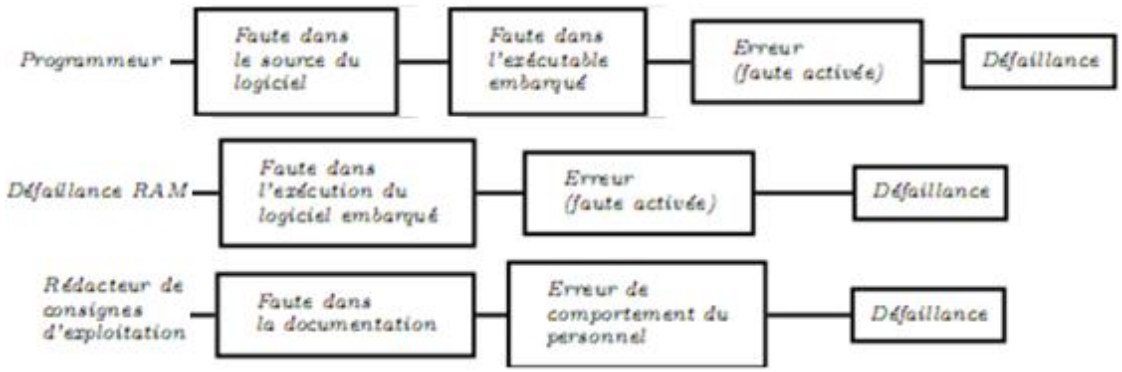


**Figure 2** : *Trois exemples d'occurrence de défaillances*

**Analyse préliminaire des dangers**

L'analyse préliminaire des dangers a été utilisée aux Etats-Unis les années 60 dans le cadre de l'analyse de sécurité de missiles. Elle a ensuite été formalisée par l'industrie aéronautique. L'analyse se fait en phase amont de conception.

L'objectif est d'identifi**er** les Dangers d'un système et leurs causes puis d'évaluer la gravité des conséquences liées aux Situations dangereuses.

L'identification des dangers est effectuée à l'aide de l'expérience et du jugement des ingénieurs, aidés de liste-guides. Les étapes de cette analyse sont:

1. Identification du contexte opérationnel dans lequel évolue le système.
2. Identification des dangers potentiels et de la sévérité de leurs conséquences.
3. Définitions d'actions correctives.
4. Vérification de la liste des conditions de panne issue de l'analyse de risque et celles des exigences de sécurité.
5. Evaluation de l'atteinte des objectifs de **SdF**.

**Eléments constitutifs de la SdF**

La démarche et le raisonnement de la **SdF** s'appuient sur des grandeurs précisées dans ce qui suit par différents auteurs définissent la **SdF** comme:

- La «**Fiabilité, Disponibilité, Maintenabilité** et **Sécurité**» qu'on retrouve dans l'acronyme **FDMS** (**RAMSS** en anglais), fait référence aux définitions de ces termes et met en avant leur complémentarité. Si la fiabilité, la maintenabilité, la disponibilité ou la sécurité ont aussi des performances d'un système, la **SdF** ne se réduit pas uniquement à une des ces performances, elle se construit par toutes ces performances [***Fournier***, 1993].

- La «**science des défaillances**» suppose la connaissance, l'évaluation, la prévision, la mesure et la maîtrise des défaillances. Ainsi la sûreté de fonctionnement apparaît davantage comme l'aptitude d'une entité à satisfaire une ou plusieurs fonctions requises dans des conditions données [***Villemeur***, 1988].

- La «**confiance justifiée dans le service délivré**» dépend principalement de la perception des utilisateurs. Le service délivré par un système est son comportement perçu par son, ou ses utilisateurs, sachant qu'un utilisateur est un autre système (humain ou physique) [***Laprieetal***., 1995].

- Le «**maintien de la qualité dans le temps**» prend en compte la conformité aux exigences (explicites ou non). Elle présente le défaut de laisser supposer qu'une activité SdF se conduit nécessairement dans le cadre d'une démarche qualité, ce qui est insuffisant [***Mortureux***, 2001].

La **SdF** est considéré comme la conjugaison de ces quatre définitions.

Les principales grandeurs de la **SdF** examinées par [***Villemeur***, 1988] sont :

- La fiabilité ;
- La disponibilité ;
- La maintenabilité ;
- La sécurité ;
- La durabilité ;
- La continuabilité ;
- La serviabilité.

**Méthodes d'analyse de la fiabilité d'un système complexe**

Dans le processus de développement de systèmes complexes, la fiabilité est devenue une caractéristique essentielle [***Mortureux***, 2001]. Ainsi, afin d'optimiser le développement de ces systèmes, il est impératif de disposer de méthodes permettant d'évaluer la fiabilité en cours de développement.

Les méthodes d'analyse de la fiabilité d'un système complexe sont nombreuses, présenter par le tableau 4.

**Tableau 4** *Principales démarches et méthodes de fiabilité*

| **Démarches/ Méthode** | **Objectif visés** |
|---|---|
| Analyse préliminaire de risque (**APR**) | Repérer a priori les risques à étudier. |
| Analyse des modes de défaillance de leurs effets et leurs criticités (**AMDEC**) | Évaluer les conséquences des défaillances |
| Arbre de défaillances (**AdD**) | Évaluer les scénarios d'un Evénement redouté |
| Diagramme de Fiabilité (**DF**) | Représenter un modèle du système à partir de la fiabilité des composants |
| Méthode de l'Espace des Etat (**MEE)** | Repérer le passage par les états de défaillance sur le fonctionnement du système |
| Réseaux de Petr (**RdP**) | Repérer le passage par les états de défaillance Sur le fonctionnement du système |
| Arbre d'événement (**AE**) | Évaluer les conséquences possible d'un événement |
| Méthode des Combinaisons de Pannes Résumée (**MCPR**) | Déterminer les combinaisons de défaillances |
| Méthode de Diagramme Causes-Conséquence (**MDCC**) | Analyse d'un événement initiateur |
| Table de Vérité (**TV**) | Recenser toutes les combinaisons d'état |

Nous avons caractérisé chaque démarche ou méthode étudiée selon trois critères [***Mortureux***, 2001]:

– méthode inductive ou déductive;
– méthode quantitative ou qualitative;
– les objectifs recherchés.

Les méthodes les plus utilisées, **APR**, **AMDEC**, **AdD**, **DF**, **MEE**, **RdP**, sont présentées ci-dessous. D'autres méthodes tel que, **AE**, **MCPR**, **MDCC**, **TV**.

**APR** (Analyse Préliminaire des Risques) : est une méthode couramment utilisée pour l'identification des risques d'un système complexe et pour l'évaluation de la gravité des conséquences liées aux risques [***Villemeur***, 1988], [***Zwingelstein***, 1996], [***Moreletal***, 1992]. L'**APR** est utiliser dès les premières phases de la conception et de compléter cette analyse jusqu'à la fin du système [***Villemeur***, 1988]. L'**APR** a pour objectifs:

– L'identification des dangers et de leurs causes (entités dangereuses, situations dangereuses, accidents potentiels,...);
– L'évaluation et l'acceptation des risques permettant une hiérarchisation;
– La proposition de mesures propres à réduire et à contenir les risques à des niveaux acceptables.

Cette démarche **APR**, ou la variante analyse préliminaire des dangers **APD**, est une étape indispensable lors que des questions de sécurités ont posées. Elle l'est beaucoup moins s'il n'est question que de la fiabilité, maintenabilité ou disponibilité. Quand elle est réalisée dès le début du projet, dès la première phase de développement du système, elle sert de référence tout au long du projet.

L'avantage de l'Analyse Préliminaire des Risques est de permettre un examen relativement rapide des situations dangereuses dans des systèmes complexes.

L'**APR** ne permet pas de caractériser l'enchaînement des évènements susceptibles de conduire à un accident majeur pour des systèmes complexes. Elle permet d'identifier des points critiques devant faire l'objet d'études plus détaillées.

L' **APR** est basée sur la liste d'éléments qui peuvent conjuguer pour Provoquer un accident entités dangereuses, situations dangereuses, accidents potentiels,...

Les résultats de l'analyse ont présentés dans un tableau à l'aide de la liste des éléments dangereux. Dans le tableau I.2 a été présenté une partie d'une **APR** sur l'électrovanne de l'**ABS**. Le domaine de la **SdF**, reprend les concepts généraux dont:

- ***Disponibilité***: Accessibilité en continue du système ;
- ***Fiabilité***: Continuité du service ;
- ***Confidentialité*** : Non-divulgation d'information ;
- ***Intégrité*** : Impossibilité d'altération des informations ;
- ***Maintenabilité*** : Possibilités de réparation et d'évolution ;
- ***Sécurité-innocuité*** (safety): Absence de conséquences.

**Les démarches inductives ou déductives**

Se basent sur celles développées dans les approches d'analyse inductive ou déductive des risques. Par exemple les méthodes :

**AMDEC** est une méthode d'analyse inductive car elle part des défaillances de composants pour en déterminer les conséquences.

**MAC** est une approche déductive car elle se focalise sur les événements redoutés d'abord pour identifier leurs causes ensuite.

**Approche de la SdF**

* Eléments prise en compte :

- De l'architecture des systèmes (Série, Redondance) ;
- Du retour d'expérience (Fréquences, Probabilités)
- Des effets des défaillances (Gravité, Criticité) ;
- Des couts (Conception, Exploitation, soutien)

* La **Sdf** est utilisable pour tous les systèmes et moyens de production

* Les méthodes et les outils de la **Sdf** sont faciles a mettre en place ;

* Les études de la **Sdf** facilitent la conception, l'exploitation et le soutien.

* L'état d'esprit général de la sureté de fonctionnement est caractérisé par une approche très « positive » qui permet d'améliorer les performances ou d'optimiser des choix de conception ou de maintien a partir d'analyses dysfonctionnelles qui sont des approches pouvant apparaitre comme étant plutôt « négatives » au départ.

# Concept FMDS

Pour étudier la **SdF** d'un système, on évalue ses propriétés. Pour un composant technique, on s'attachera à étudier:

## *1 - Fiabilité*/ reliability

***a) Définition :*** Capacité (aptitude) d'un système (dispositif) à accomplir la fonction requise dans des conditions données, dans une durée donné.

***b) Mesure :*** La fiabilité est caractérisée par la probabilité qu'un système S accomplisse une fonction requise dans des conditions données, dans un intervalle de temps **[0;t]** sachant que l'entité n'est pas en panne à l'instant **0**.

**R(t) = P** (**S** non défaillant sur **[0;t])** (I.1)

Où **S** est un système (entité, composant, fonction). On peut expérimentalement calculer cette probabilité. On prend **n** composants identiques qui fonctionnent a **t=0**, et on compte a chaque instant $\mathbf{t}_i$ combiens ont il toujours en marche **v(t)**. Alors, **R(t) = v(t) = n**

Nous admettrons par la suite que le temps est la variable principale dont dépend la fiabilité. Pour certains appareils, il peut être plus judicieux de prendre une autre variable: nombre de cycles d'ouverture-fermeture pour un relais, nombre de tours pour un moteur, nombre de kilomètres pour une voiture, etc.

Soit **T** la variable aléatoire mesurant la durée de fonctionnement de l'entité, on a :

$$\mathbf{R(t)} = P\,[T>t].$$

La défiabilité

$$\bar{\mathbf{R}}\mathbf{(t)} = 1 - R(t)$$

Est donc égale a la fonction de répartition de **T,** $\bar{\mathbf{R}}\mathbf{(t)} = F(t)$

***Fiabilité humaine***

La fiabilité humaine concerne la tâche plutôt que la fonction. La tâche et la fonction renvoient à une notion commune : le but à atteindre. La fonction est liée à l'objectif du procédé piloté, c'est-à-dire au service rendu par celui-ci, la tâche est liée à l'objectif du moyen technique ou humain qui réalise cette fonction. Pour réaliser une fonction donnée, le comportement humain est subordonné à une prescription appelée tâche et ce qui est mis en œuvre pour la réaliser est l'activité.

Une erreur humaine renvoie alors à une dérive entre tâche effective, modèle issu de l'analyse de l'activité, et tâche prescrite, modèle de ce qui devrait être réalisé. Toutefois, l'omission d'une tâche peut être assimilée à une cessation de l'aptitude humaine et la réalisation incorrecte d'une tâche à une altération des capacités humaines.

Les notions d'erreur et de défaillance humaines peuvent donc être confondues, et les concepts d'erreur ou de fiabilité humaines se rattachent à la capacité d'un opérateur humain à réaliser ses tâches respectivement avec ou sans dérives de comportement.

La fiabilité humaine est donc relative à l'exécution correcte de l'ensemble des tâches de l'opérateur regroupant les tâches de surveillance du comportement d'un procédé donné, les tâches de contrôle de la sécurité du système homme-machine, les tâches de prévention et de récupération d'erreur humaine ou technique. En prenant en compte les contraintes d'interaction avec les tâches des autres opérateurs humains et celles des systèmes automatisés au travers d'interfaces de dialogue homme-machine, un opérateur humain doit par conséquent :

- Prendre les décisions adéquates pour optimiser le fonctionnement du procédé ;
- Récupérer les dérives anormales de fonctionnement du procédé ou de lui-même, en particulier celles que le système automatisé ne sait pas prendre en compte ;
- Contrôler les risques associés à ces dérives sans obligatoirement tenter de les récupérer mais en adaptant les modes opératoires initiaux ;
- Eviter l'occurrence d'événement catastrophique dû à ces dérives ;
- Réguler son activité afin d'être prêt à réagir ou de maintenir ses connaissances.

Ainsi, la fiabilité humaine est définie comme la capacité humaine à réaliser les tâches requises correctement et ne pas réaliser d'autres tâches nuisibles au bon fonctionnement du procédé. L'erreur humaine est son complémentaire : c'est la capacité humaine à ne pas réaliser les tâches prescrites correctement ou à réaliser d'autres tâches nuisibles au bon fonctionnement du procédé.

## 2 - ***Disponibilité*** / Availability)

***a) Définition:*** Capacité (aptitude) d'un système (entité) à réaliser ces fonctions requises dans des conditions données, a un temps donné. En supposant que la fourniture des moyens extérieurs soit assurée.

***b) Mesure :*** La disponibilité est caractérisée par la probabilité ***D(t)*** qu'un système **S** soit en état d'accomplir une fonction dans des conditions données, a un temps donné.

$$D(t)=P\ (S \text{ non défaillant à l' instant } t) \qquad (I.2)$$

C'est une grandeur instantanée, le système peut subir des pannes et réparations avant **t**.

## 3 - ***Maintenabilité*** / Maintainability

***a) Définition*** : Aptitude (capacité) d'un composant à être maintenu ou réparé sur un intervalle de temps donné, afin de pouvoir réaliser ces fonctions. Lorsque la maintenance est accomplie dans des conditions données avec des procédures et des moyens prescrits, selon un programme.

***b) Mesure :*** La maintenabilité est caractérisé par la probabilité **M (t)** que la maintenance d'un système **S** réalisé dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps **t**, système défaillant à **t=0**.

**M(t)=P (S** est repéré sur **[0; t]**). (I.3)

Soit Y la variable aléatoire désignant la durée de la panne du composant, alors :

**M(t) = P (Y ≤ t)**.

La densité de réparation est : **G (t)= dM (t) / dt** .

Ainsi, **G(t) dt** est la probabilité que la réparation soit achevée dans l'intervalle [**t;t + dt**] sachant que l'entité est défaillante a **t = 0**.

## 4 - *Sécurité* / Safety

***a) Définition***: capacité (aptitude) d'un composant (système) d'éviter l'occurrence d'un fait catastrophique dans des conditions des événements critiques ou catastrophiques.

***b) Mesure*** : La sécurité est caractérisée par la probabilité **S (t)** qu'un système **S** évite de faire apparaitre, dans des conditions, des événements critiques ou catastrophiques.

Les caractéristiques d'un opérateur humain peuvent être assimilées à celles des composants techniques. Toutefois, en général, la notion de fiabilité humaine est aux facteurs humains ce que la sûreté de fonctionnement est aux facteurs techniques.

**S (t)= P** (**E** évite des évènements critiques ou catastrophiques sur **[0, t]**)

## 5 – Risque :

Le risque relatif au phénomène dangereux considéré est une fonction de la gravité du dommage possible pouvant résulter du phénomène dangereux considéré et de la probabilité d'occurrence du dommage.

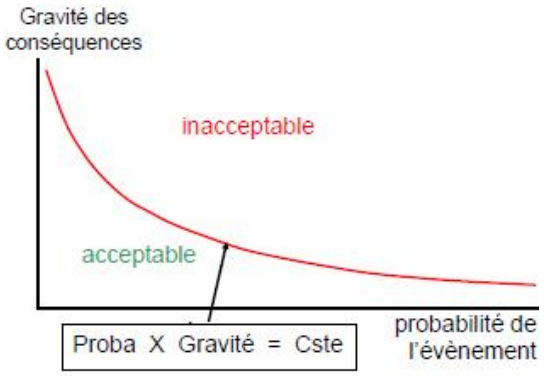


**Figure :** *Acceptation du risque*

# METHODE D'ANALYSE

1- **Analyse Fonctionnelle (AF)**

A/ Analyse Fonctionnelle Externe (AFE) : Elle permet de définir avec précision :

- Les limites fonctionnelles et matérielles du système ;
- Les différentes fonctions et missions réalisées par le système ;
- Les diverses configurations d'exploitation.
- Limites du système et configurations d'exploitation
- Définition des fonctions (principales et contraintes)

B/ Analyse Fonctionnelle Interne (AFI) : Elle permet :

- de réaliser une décomposition arborescente et hiérarchique du système en éléments fonctionnels et/ou matériels ;
- De lister le cheminement des fonctions définies au niveau système au travers des différents éléments.
  - Décomposition matérielle en équipements ;
  - Précision des fonctions de chaque équipement

2- **Analyse quantitative** ;

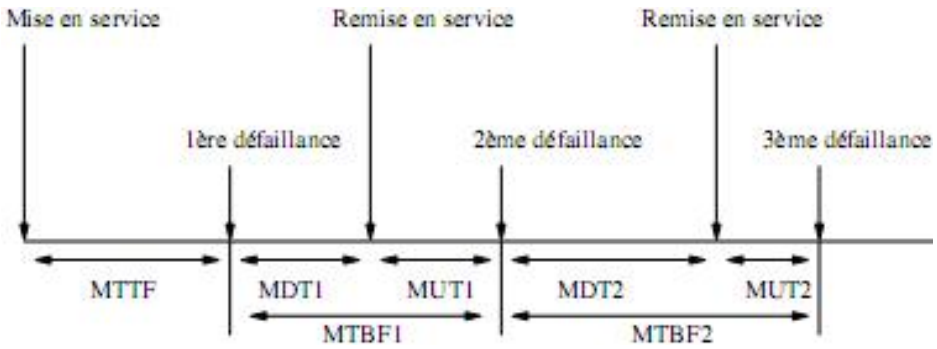


**Figure 3 –** *Représentation des temps moyens dans la vie en opération.*

Ou: **MTBF = MUT + MDT**.

Tel que :

- **MTBF** (Mean Time Between Failure): durée moyenne entre deux défaillances consecutives d'un équipement réparé (pannes) ;

- **MDT** (Mean Down Time): durée moyenne de non fonctionnement du système ;

**- MUT** (Mean Up Time): durée moyenne de fonctionnement du système après réparation ;

**- MTTR** (Mean Time To Repair ; Restoration): (durée moyenne de fonctionnement d'un équipement avant la première défaillance) ;
**- MTTF** Mean Time To Failure (durée moyenne de fonctionnement d'un équipement avant la première défaillance) ;

En utilisant la loi exponentielle (taux de défaillance constant). On obtient :
- *Taux de défaillance* : **$\lambda$=1/MTTR** si **MTTR « MTTF** .
Si **MTTF » MTBF** alors **$\lambda$=1/MTBF**.
- *Taux de réparation* : **$\mu$=1/MTTR**.

3- **Analyse Préliminaire des Risques (APR)** ;
Analyse réalisée des le début d'une étude ;

Etablir la liste aussi exhaustive que possible des incidents/ accidents pouvant avoir des conséquences sur la sécurité du personnel et du matériel.

4- **Diagrammes de Fiabilité (DdF)** ;

**Objectif** :
Représentation de la structure du système et calculs de la fiabilité, de la maintenabilité et de la disponibilité du système. En introduisant les données quantitatives de chaque élément (taux de défaillance et taux de réparation), il est possible de déterminer :
* La Fiabilité du système
- Courbe de fiabilité du système en fonction du temps
- **MUT** : Mean Up Time (Temps de disponibilité du système)
* La maintenabilité du système
- Courbe de maintenabilité du système en fonction du temps
- **MDT** : Mean Down Time (Temps d'indisponibilité du système)
* La disponibilité du système
- Courbe de disponibilité du système en fonction du temps
- Disponibilité Moyenne = **MUT** / (**MUT** + **MDT**).

## 5- Analyse des Défaillances (AMDEC)

### Objectif

Analyse des Modes de défaillance, de leurs Effets et de leurs Criticités, l'**AMDEC**, précédée d'une Analyse fonctionnelle, a pour objet l'obtention de la fiabilité optimale d'un système ou d'un moyen de production. Elle permet de lister et classifier les défaillances des équipements du système.

### Méthode

* Recherche des défaillances des éléments du système ;
* Identification des causes possibles ;
* Evaluation des effets Des défaillances ;
* Estimation du risque (Criticité) ;
* Recherches d'amélioration ;
* Mise en œuvre des amélioration.

Indice de criticité : $C = P \times G$

C > Seuil → Amélioration → Diminution de la probabilité d'apparition des dysfonctionnements et de la gravité de ses effets.

**Tableau 5 -**

| Rep | EQUIPEMENT | FONCTION | MODE DE DEFAILLANCE | CAUSE | EFFET | P | G | C | AMELIORATIONS |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | |
| | | | | | | | | | |

Hiérarchisation des dysfonctionnements en fonction de leur Criticité (C) qui tient au moins compte de:

P : Probabilité d'apparition des dysfonctionnements

G : Gravité des effets des dysfonctionnements

## 6- Analyse de Maintenance

**Tableau 6 -**

| Rep | Description de la tâche | Niveau | Périodicité | Durée | Personnel | Outillage | Rechange | Ef. | Co. | I | Choix |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |

Hiérarchisation des tâches de maintenance en fonction de leur Intérêt (I) qui tient au moins compte :

Ef : Efficacité a priori de la tâche

Co : Estimation du coût de la tâche

**Objectif :**

L'analyse de maintenance, précédée d'une AMDEC, permet de préconiser au plus juste les interventions de maintenance préventive pour chacun des éléments du système.

**Méthode :**

- Préconisation des taches de maintenances préventive ;
- Description des taches: Niveau, Périodicité, Durée, Personnel, Outillage, Rechanges…;
- Eventuellement : Cotation et hiérarchisation vis-à-vis de l'intérêt des taches (Efficacité, Cout…) ;
- Elaboration du plan de maintenance préventive.

La synthèse de l'analyse de maintenance comprend :

- Le calendrier des interventions préventives ;
- Les besoins en personnel ;
- Les listes des outillages et des équipements de testes ;
- Les infrastructures nécéssaires ;
- Les stocks de pièces de recharge ;
- Le plan de maintenance préventive ;
- Les couts de maintenance.

7- **Arbres de Défaillance (AdD)**.

**Objectif** :

Mise en évidence des diverses combinaisons possibles d'événements qui entraine la réalisation d'événements redoutés. Représentation des combinaisons au moyen d'une structure arborescente.

**Analyse qualitative :**

- Détermination des coupes minimales (chemins critiques) ;
- Une coupe minimale est une combinaison d'évènements élémentaires entrainant l'évènement redouté, tel qu'aucun sous ensemble de cette combinaison ne produise cet évènement redouté.

**Analyse quantitative**

- Calcul de la probabilité d'occurrence des évènements redoutés pour un temps de mission donné à partir des probabilités d'occurrence de chaque événement.

# PLAN SdF

**Objectif :**

Présenter les dispositions par le maitre d'œuvre en matière de **SdF**, pour répondre aux exigences exprimées dans les spécifications de besoin.

**Moyen :**

Décrire les exigences de la **SdF**, la stratégie mise en œuvre (management), les méthodes utilisées, les procédures appliquées pour concevoir et assurer la **SdF**.

**Exemple de plan SdF :**

1/ Introduction ;
2/ Description du système et de son utilisation ;
3/ Exigences SdF et hypothèses ;
4/ Organisation mise en place
5/ Taches de management de la SdF ;
6/ Description des taches ;
7/ Méthodologies d'analyses appliquées ;
8/ Planification des taches.

## Etude des systèmes

Un système peut être décrit comme un ensemble d'éléments en interactions entre eux et avec l'environnement dont le comportement dépend :

- Des comportements individuels des éléments qui le composent ;
- Des règles d'interactions entre éléments (interface) ;
- De l'organisation topologique des éléments (Architecture).

**Exemple :**

Une installation chimique, une centrale nucléaire ou un avion ont 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 donnes. Tous les systèmes nécessitent un recours aux concepts et aux techniques de la **SdF**, depuis la préparation et la conception, jusqu'à la réalisation l'utilisation et le soutien. L'objet d'étude de la **SdF** est la fonction. Une fonction peut être définie comme l'action d'une entité ou de l'un de ses composants exprimées en termes de finalité. On distingue les fonctions et la structure. La figure 4, représente la description fonctionnelle d'une machine à laver :

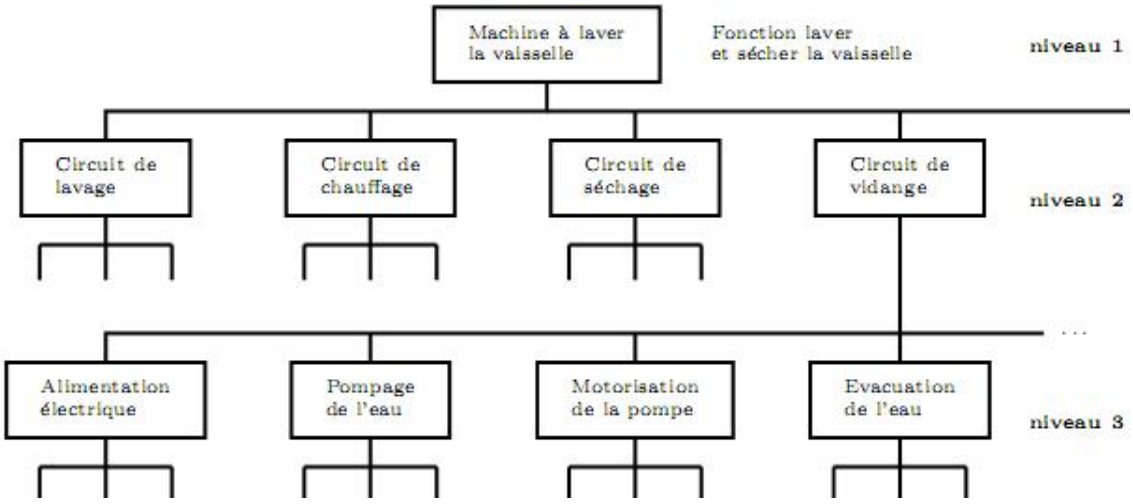


**Figure 4 –** *Description fonctionnelle d'une machine à laver la vaisselle.*

- fonction principale: raison d'être d'un système (pour un téléphone portable, la Fonction principale est la communication entre deux entités);

- fonctions secondaires: fonctions assurées en plus de la fonction principale (horloge, réveil, jeux...);
- fonctions protection: Assurer la sécurité des biens des personne et environnement;
- fonctions redondantes: plusieurs composants assurent la même fonction.
- Une description fonctionnelle qui se fait par niveau (arborescence hiérarchisée).

## Structure du système

Les fonctions sont réalisées par le système à partir de ses composants. La structure du système doit être prise en compte pour les analyses de la **SdF**. Pour cela, il faut décrire les composants matériels, leur rôle, Leurs caractéristiques et leurs performances.

On peut utiliser une description en niveau. La figure 5 identifie les composants intervenant dans la structure de la machine à laver.

Il faut également décrire les connexions entre composants, ce qui peut être fait par un graphe oriente pour lequel l'ensemble des nœuds désigne l'ensemble de n ressources connectées entre elles par des liaisons représentées par les arcs.

En fin, il est également important dans certains cas de préciser la localisation des composants. Les analyses de La **SdF** reposent sur des hypothèses au sujet de l'indépendance des défaillances des fonctions élémentaires. Le partage de ressources et l'installation de ces ressources dans une même zone risquent de violer les exigences d'indépendances. Par exemple, un éclatement pneu dans un avion peut entrainer. La défaillance de plusieurs composants.

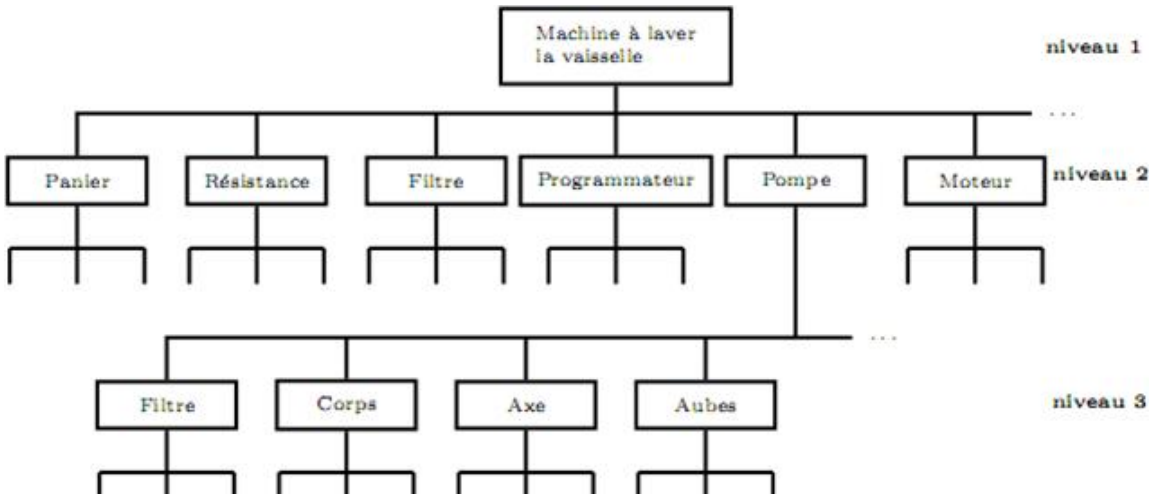


**Figure 5** - *Décomposition matérielle d'une machine à laver la vaisselle.*

La **SdF** manipule un certain nombre de concepts dont:

### a) Système cohérent:

Un système est dit cohérent si:

- La panne de tous les composants entraine la panne du système ;
- Le fonctionnement des composants entraine le fonctionnement du système ;
- Lorsque le système est en panne, aucune défaillance supplémentaire ne rétablit son Fonctionnement;
- Quand le système est en marche, aucune réparation n'induit sa panne.

### b) Les attributs de la sureté de fonctionnement

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

. La fiabilité est la continuité du service ;
. La disponibilité est le fait d'être prêt à l'utilisation ;
. La maintenabilité est l'aptitude à être réparé ;
. La sécurité est l'aptitude à ne pas provoquer d'accidents catastrophiques.

On suppose que le système se met en fonctionnement à l' instant t=0 et ne présente qu'un seul mode de défaillance.

Le composant fonctionne pendant un temps aléatoire $X_1$ au bout duquel il tombe en

panne. Il y reste pendant un temps aléatoire $Y_1$ durant son remplacement puis est remis en fonctionnement et ainsi de suite. On dit que le système est réparable. Lorsque le composant n'est jamais réparé, on dit qu'il est non réparable. La description graphique du comportement du système est donnée à la figure 6

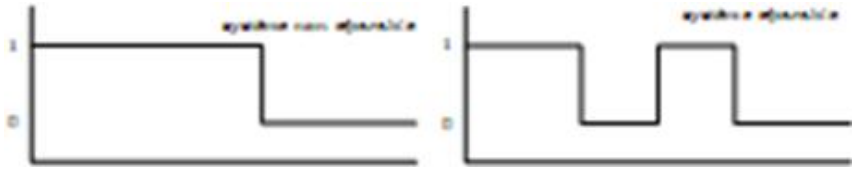

**Figure 6 :** *comportement du système*

**<u>Autres attributs :</u>**

D'autres attributs de sureté de fonctionnement ont été identités. Comme par exemple la testabilité (testability) qui est le degré d'un composant ou d'un Système à fournir des

informations sur son état et ses performances, ou la sécurité (sécurity) qui la disponibilité pour les usagers autorisés seulement, la condentialité et l'intégrité...

**Les moyens de la SdF**

Propriété d'un système telle que ses utilisateurs puissent placer une confiance justifiée dans le service qu'il délivre.

**A- Fourniture de la sureté de fonctionnement**

C'est la tolérance aux fautes et leur prévention c'est a dire Tendre vers un système exempt de fautes ou défaillances.

***Empêcher*** (prévention des fautes) par construction. Occurrence des fautes ;

***Délivrer*** (Tolérances aux fautes) par redondance. Service conforme a fonction du système en dépit des fautes. Délivrer un service ou accomplir la, ou les fonctions du système en dépit des fautes selon :

**a/ Détection d'erreurs**

Identifier la présence d'un état erroné :

- sans interruption de service : composant autotestable
- préemptive

**b/ Rétablissement système**

Transformer un état erroné en état exempt d'erreur détectée et de faute qui puisse être activée à nouveau selon :

***Traitement d'erreur***: Eliminer les erreurs du système, avant défaillance ;

***Traitement de fautes***: Éviter que les fautes ne soient activées à nouveau.

Facteurs à prendre en compte pour la tolérance aux fautes :

- *Attributs de sûreté de fonctionnement*: disponibilité, sécurité innocuité, etc.
- *Classes de fautes* : permanentes/transitoire accidentelles/malveillantes, physiques/conception, (solides/douces), etc.
- *Nombre de fautes à tolérer* (k) : degré de redondance (k)
- *Durée maximale d'interruption de service.*

***B-* Analyse de la sureté de fonctionnement**

Avoir confiance dans l'aptitude du système à fournir un service conforme a l'accomplissement de sa fonction selon :

***Minimiser*** (Elimination des fautes) par vérification. Présence des fautes.

***Prévoir*** (Prévention) par évaluation. Présence, création et conséquences des fautes.

**Entraves**

Circonstances indésirables (non-attendues) causes ou résultats de la non sûreté de fonctionnement *(confiance ne peut plus être placée dans le service délivré)*

**Moyens**

Méthodes, outils et solutions pour procurer au système l'aptitude à délivrer un service sur lequel on puisse placer sa confiance, et pour avoir confiance dans cette aptitude.

**Attributs**

Permettent :

a) d'exprimer les propriétés attendues du système ;

b) d'apprécier la qualité du service, telle que résultant des entraves et des moyens de s'y opposer.

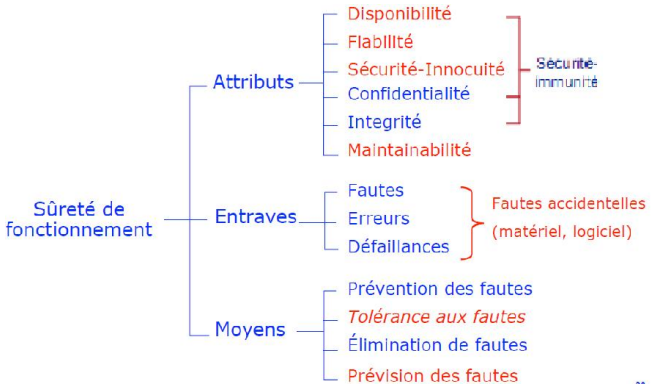


**Figure 7 –** *Résumé sur les premières notions*

Dans figure 7, sont résumées les différents notions déjà rencontrées. Les entraves sont les défaillances et leurs causes, les attributs de sureté de fonctionnement ont été étudiés dans la partie précédente. Dans cette partie, nous illustrons les moyens pour concevoir des systèmes surs de fonctionnement.