Sûreté de Fonctionnement

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.

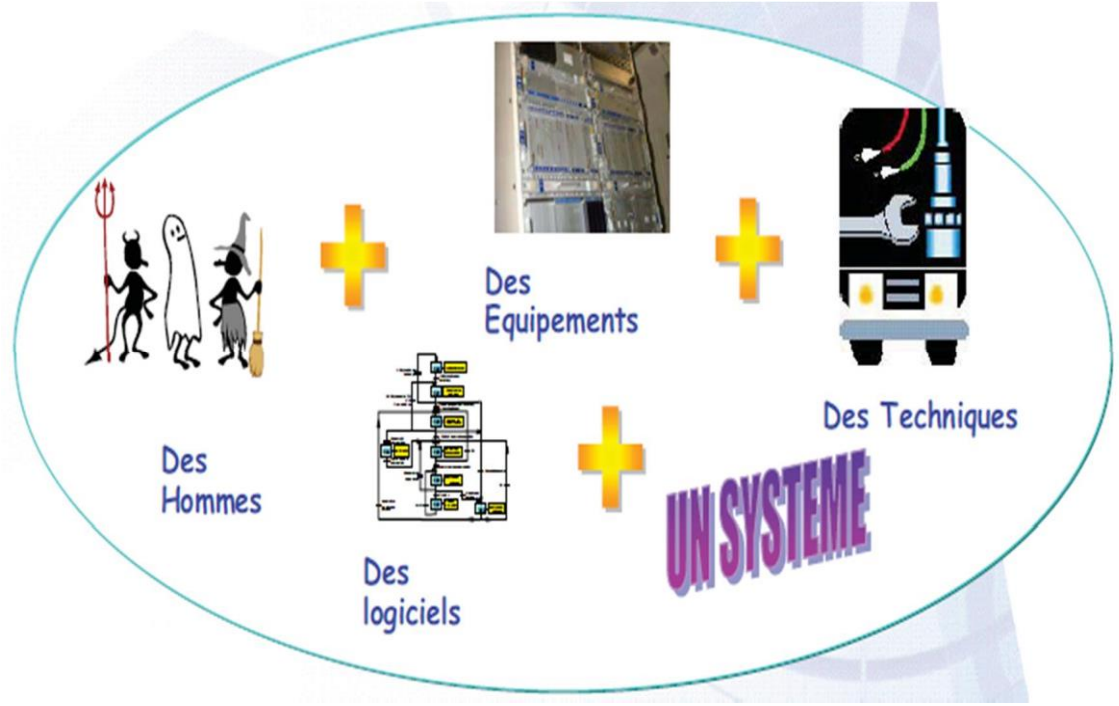
1. Introduction

Objectif de la sûreté de fonctionnement (SdF):

L'objectif de la SdF est d'atteindre l'idéal de la conception de **système**: zéro **accident**, zéro **arrêt**, zéro **défaut** (et même zéro **maintenance**).

La SdF 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.

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.

Exemple1 : Uneampoule électrique

- Quellessont sesparties essentielles?
- Quelestlecomportementattendu?

Une ampouleélectrique.

Composée d'une enveloppe en verre, d'un lament, d'une douille.

Comportement attendue

1. Si l'ampoule est sous tension,alors elle doit éclairer.

- Celasembleune évidence...
- Cette phrase est-elle suffisamment précise ?
- Pendant combien detemps?
  Notionde «**durée acceptable**»

2. qu'elle soitou non sous tension,elle ne doit pas être dangereuse

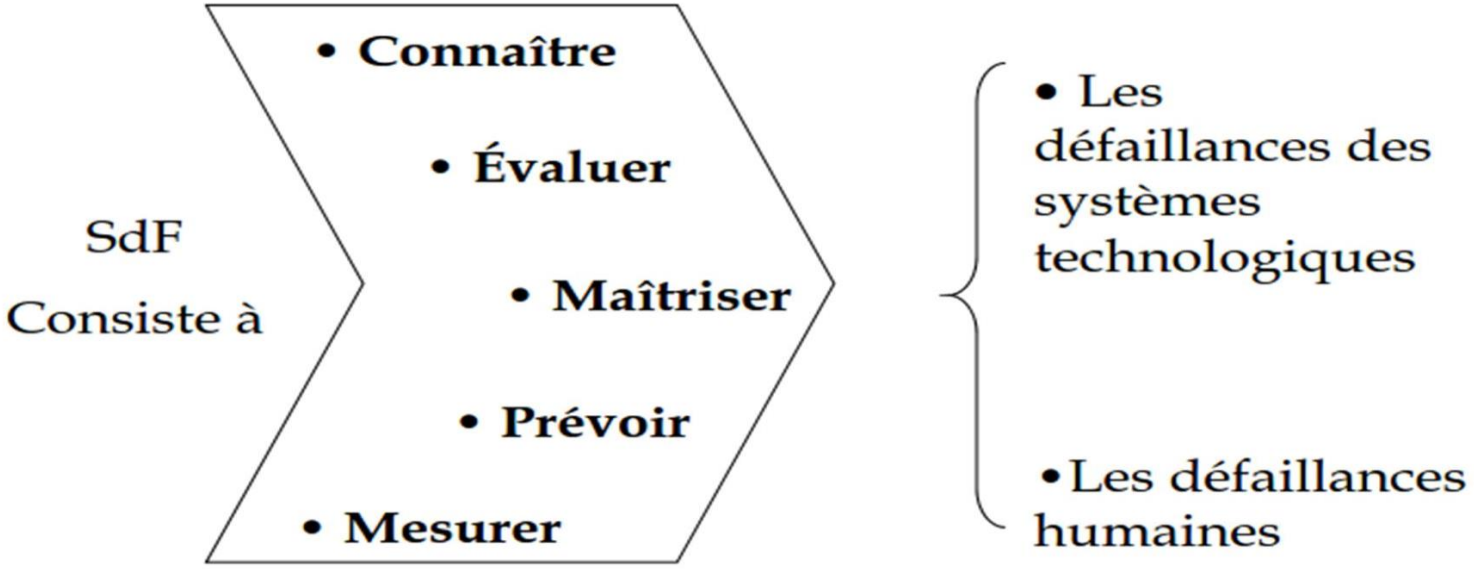
- Résistance de l'enveloppe à la chaleur dégagée, refroidissement rapide,
- Bonneisolation électrique:propriété en **fonctionnementnominal**
- Résistanceauxsurtensions:propriétéen**fonctionnementtemporaire**
- Arrêtdéfinitifne doit pasavoirdeconséquencesgraves: **fonctionnement dégradéacceptable**
  Ces **exigences** font partie du **cahier des charges**.

Mais encore...

3. Taille et forme appropriées à une série d'utilisations possibles...

2. Concepts

2.1. Les enjeux de la sûreté de fonctionnement



2.2. Définitions

La sûreté de fonctionnement (dependability)

La propriété qui permet à ses utilisateurs de placer une **confiance justifiée** dans le **service** qu'il leur délivre.

Définition selon la norme CEI50 (191):

La sûreté de fonctionnementest l'aptituded'une entité à assumer une ou plusieurs fonctions requises dansdes conditions données.

Définition selon la norme CEI 50 (191) :

La sûreté de fonctionnement est l'aptitude d'une **entité** à assumer une ou plusieurs **fonctions** requises dans des conditions données.

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 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

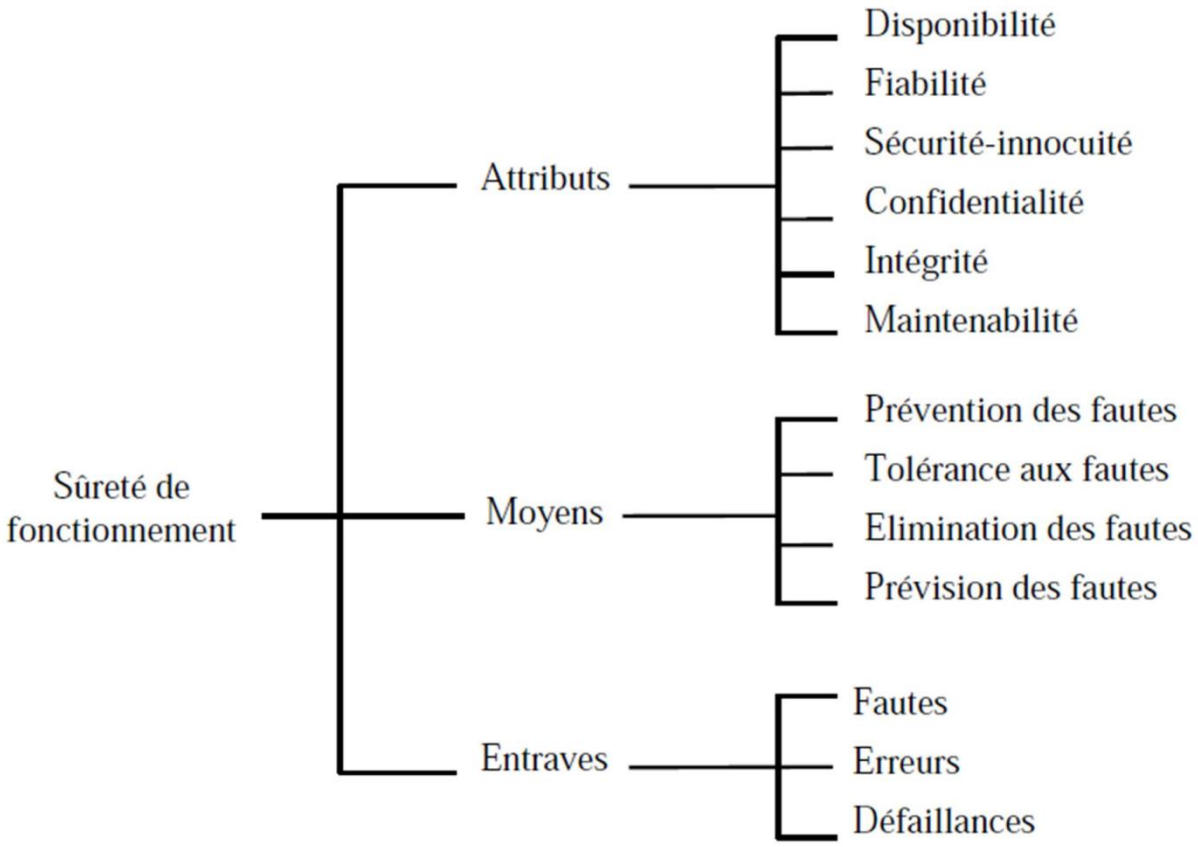
La partie de la frontière du système où ont lieu les interactions avec ses utilisateurs.

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.



2.3. Composantes de la SdF

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

FMDS & Sdf

- Fiabilité
- Maintenabilité/ Maintenance
- Disponibilité
- Sécurité/Sûreté

- Evaluée par ses composantes FMDS
- Approche probabiliste

1. Fiabilité

- La fiabilité est l'aptitude d'un dispositif à accomplir une fonction requise, dans des conditions d'utilisation et pour une période de temps déterminée.

- Le terme « fiabilité » est utilisé comme une caractéristique indiquant une probabilité de succès.

(Extrait de NF X 06-501)

Exemples :

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

2. Maintenabilité/ Maintenance

- Dans des conditions données d'utilisation, la maintenabilité est l'aptitude d'un dispositif à être maintenu ou rétabli dans un état dans lequel il peut accomplir sa fonction requise, lorsque la maintenance est effectuée dans des conditions données avec des procédures et des moyens prescrits.
- Le terme « maintenabilité » est aussi défini comme une caractéristique indiquant une probabilité pour que le dispositif soit réparé dans un intervalle de temps donné.

(Extrait NF X 60-010)

3. Disponibilité

- Aptitude d'un dispositif (équipement, système, service,…), sous les aspects combinés de sa fiabilité, de sa maintenabilité et de la logistique de la maintenance, à remplir ou à être en état de remplir une fonction à un instant donné ou dans un intervalle de temps donné.

(Extrait NF X 60-503)

4. Sécurité

- Aptitude d'un système à ne pas générer, dans des conditions données, des événements critiques ou catastrophiques.
- Probabilité que le système évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

Sécurité d'une machine

- Aptitude d'une machine à accomplir sa fonction, à être transportée, installée, mise au point, entretenue et mise au rebut dans les conditions d'utilisation normale spécifiées dans la notice d'instructions, sans causer de lésion ou d'atteinte à la santé.

(Extrait de EN 292-1)

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.
(Extraits de EN 1050)

3. Les moyens de la sûreté de fonctionnement

3.1. 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'implantations

3.2. Tolérance aux fautes

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

3.3. 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.

3.4. Prévision des fautes

Consiste à anticiper les fautes et leur impact sur le système.

4. Entraves à la SdF

4.1. Défaillance :

Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise.

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.

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 qui entraîne la perte d'une (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 (*catastrophic*)	Défaillance qui occasionne la perte d'une (ou des) fonction(s) essentielle(s) du système en causant des dommages importants au système ou à son environnement et/ou entraîne la mort ou des dommages corporels

4.2. Erreur

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

4.3. Faute

La cause de l'erreur est une faute (par exemple : un court-circuit sur un composant).

Classification des modes de défaillance

Les modes de défaillance : sont les manières selon lesquelles un système peut être défaillant, classées selon leur gravité.

Mode de défaillance	Explication
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	

5. Etudes de sûreté de fonctionnement

- Regroupent l'évaluation prévisionnelle de la FMDS d'une organisation, d'un système, d'un produit ou d'un moyen
- Permettent, par comparaison aux objectifs, d'identifier les actions de conception ou d'amélioration de l'entité
- Peuvent également concerner le suivi des performances d'un système en exploitation
- Utilisent un ensemble d'outils et de méthodes qui consistent également à analyser les effets des pannes, dysfonctionnements, erreurs d'utilisation,…..de l'entité étudiée

5.1. Les Méthodes d'analyse de sûreté de fonctionnement

Une analyse prévisionnelle de sûreté 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 sûreté de fonctionnement (fiabilité, disponibilité, maintenabilité, sécurité). Les éléments de ce modèle seront des événements susceptibles de se produire dans le système et son environnement, tels par exemple :

- des défaillances et des pannes des composants du système,
- des événements liés 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 :

Quelques méthodes et outils de la Sdf

- Diagramme de fiabilité
- Analyse préliminaire des risques
- AMDE(C)
- Arbres de défaillance
- Graphes de markov
- ……

5.2. Démarche d'analyse de la sûreté de fonctionnement

I. Analyse de système

C'est un processus consistant en l'acquisition et le traitement d'informations relatives au système et pertinentes au regard d'une décision ou d'un objectif donné. Le résultat de cette analyse est un modèle du système.

I.1. Acquisition d'informations

Cette étape vise à collecter l'ensemble des informations pertinentes pour mener le travail d'analyse de façon efficace en suivant les étapes :

- Description technique et fonctionnelle de l'installation
- Identification des potentiels des dangers
- L'analyse des accidents survenus sur des installations similaires
- Environnement du système

I.2. Délimitation et décomposition du système

Il est important de fixer dès le début d'une étude de sûreté de fonctionnement les principales caractéristiques du système à prendre en compte, à savoir :

- **Les fonctions du système** : principales et secondaires.
- **La structure du système** : composants et leurs caractéristiques, leur rôle, relations entre les composants, leur localisation,…etc.
- **Les conditions de fonctionnement du système** : les différents états, conditions de fonctionnement des composants, changement de configuration,…etc.
- **Les conditions d'exploitation du système** :
  - Les conditions de surveillance (alarmes, inspections,…)
  - Les conditions d'intervention (maintenance,…)
  - Les spécifications techniques d'exploitation

- **L'environnement du système** :
  - Les autres systèmes de l'installation
  - L'ensemble des opérateurs humains
  - L'environnement physique
  - Les conditions météorologiques, les agressions naturelles (séismes, inondations,…) ou industrielles.

I.3. Processus d'analyse

Le processus d'analyse doit conduire à l'obtention d'un premier modèle du système ; puis après des compléments d'études et des révisions, à l'obtention d'un dernier modèle du système. Les conclusions de l'analyse ainsi que les décisions à prendre seront basées sur ce modèle.

II. Analyse de la sûreté de fonctionnement (SdF) d'un système

II.1. Prévision de la sûreté de fonctionnement

Lorsque le processus précédent est orienté vers l'obtention d'un modèle relatif à une caractérisation de la sûreté de fonctionnement (exemples : fiabilité, disponibilité, maintenabilité, sécurité), on parle d'analyse de sûreté de fonctionnement d'un système.
Les éléments de ce modèle seront des événements susceptibles de ce produire dans le système et son environnement tels que par exemples :

- Les défaillances des composants du système,
- Les événements liés à l'environnement,
- Les erreurs humaines dans la phase d'exploitation

II.2. Les méthodes d'analyse de la sûreté de fonctionnement

Afin d'aider l'analyste à établir un modèle de la sûreté de fonctionnement, des méthodes d'analyse ont été élaborées, parmi lesquelles citons :

- Analyse Préliminaire des Risques (APR)
- Analyse des Modes de Défaillance et de leurs Effets (AMDE)
- Méthode du Diagramme de Succès (de fiabilité) (MDS/MDF)
- Méthode de l'Arbre de Défaillance (AdD)
- Méthode de l'Arbre des Conséquences (ou des Evénements) (MAC/AdE)
- Méthode de l'Espace des Etats (Graphes de Markov) (MEE).

II.3. Démarche Inductive et Déductive

On distingue deux types de démarches dans l'analyse SdF d'un système : la démarche inductive et la démarche déductive.

II.3.1. Démarche Inductive : On raisonne du plus particulier au plus général.
Face à une défaillance (ou combinaison de défaillances ; on examine de façon détaillée les effets de celui-ci sur le système et/ou sur l'environnement.
Exemple : Analyse des conséquences de la rupture d'une tuyauterie du circuit primaire d'un

réacteur nucléaire est de nature **inductive**.

II.3.2. Démarche Inductive : On raisonne du plus général au plus particulier.
Supposons que le système soit défaillant, on recherche les causes de cette défaillance.
Exemple : la recherche des causes d'une explosion d'un bac de stockage est de nature **déductive**.

III. Les principales étapes d'une analyse de Sûreté de Fonctionnement

On distingue quatre étapes principales d'une analyse de SdF d'un système (Fig).

III.1. Analyse technique et fonctionnelle : Cette étape consiste à recueillir les premières informations relatives au système et à des caractéristiques techniques et fonctionnelles.
Le résultat de cette étape est l'identification et la définition des principales fonctions du système et ses limites extérieures.

III.2. Analyse qualitative : Dès le début de cette étape :

- Définir les objectifs de l'analyse de la SdF : s'agit-il d'une étude de fiabilité, de disponibilité, de maintenabilité ou de sécurité ?
- Préciser les limites de résolution de l'analyse : niveaux de décomposition du système. Le résultat est la proposition d'une décomposition du système en composants qui peut être différente de celle retenue dans la description du système.
- Rechercher les causes de défaillance par les méthodes d'analyse qualitative. Le résultat c'est la modélisation de la SdF du système et des défaillances l'affectant.

N.B :

- La modélisation de la SdF d'un système est étroitement liée à la modélisation des phénomènes physiques, qui sont un champ d'apparition des défauts du système.
- Des hypothèses spécifiques doivent être faites âr l'analyste : l'impact de l'environnement ou des autres systèmes, le comportement de l'opérateur humain, les opérations de test ou de maintenance,….

III.3. Analyse quantitative : Consiste à caractériser par des mesures (probabilités) la SdF du système, moyennant un traitement mathématique du modèle.
Les données alimentant le modèle :

- ❖ Données relatives aux composants (taux de défaillance, de réparation, probabilités de défaillance,….) ;
- ❖ Données relatives aux défaillances humaines ;
- ❖ Données relatives aux agressions de l'environnement physique.

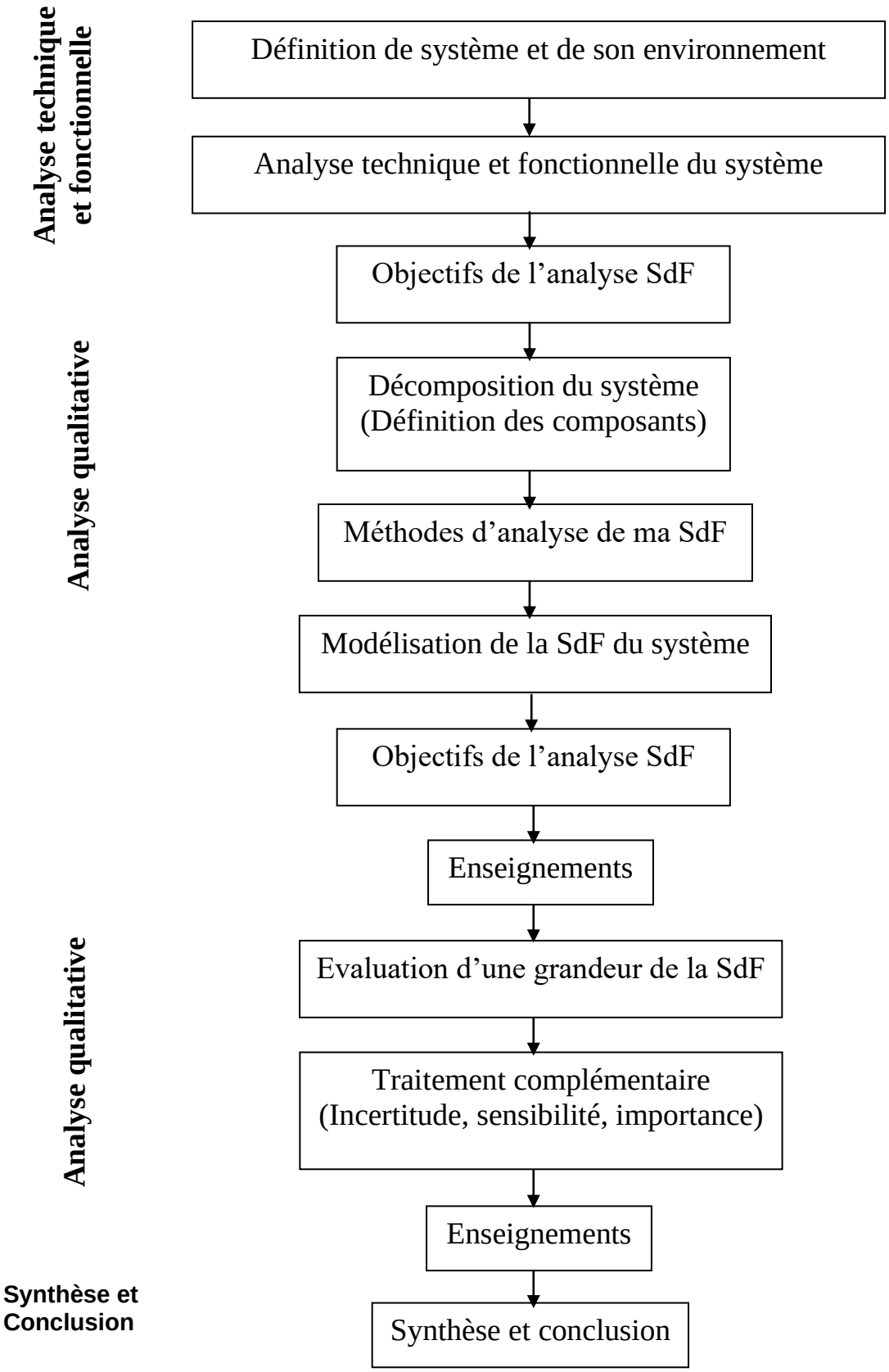


Fig . . Etapes principales de l'analyse de SdF

III.4. Synthèse et conclusion :

- La synthèse de l'analyse qualitative et quantitative mettra en évidence :
  - Les défaillances et leurs combinaisons qui compromettent la SdF du système
  - Les composants critiques du système
  - Les missions importantes
- Les conclusions permettent de considérer le système soit comme répondant aux exigences de SdF, soit comme non répondant. Dans le dernier cas, des propositions peuvent être faites. Par exemple :
  - Une amélioration de la fiabilité des composants,
  - Une redondance supplémentaire,
  - Une élimination de redondances inutiles,
  - Un ajout de protection ou de dispositif de surveillance ou de contrôle,
  - Une protection supplémentaire contre les défaillances de causes communes,
  - Des essais périodiques supplémentaires,
  - Une modification des caractéristiques des tests périodiques,
  - Une maintenance préventive,
  - Une modification des procédures d'exploitation,…

IV. Caractéristiques d'une analyse de Sûreté de Fonctionnement

IV. 1. Interactions : dans le cadre d'une analyse d'un système réel, certaines étapes s'avèrent très liées entre elles.
Pae exemples :

- La définition des composants, retenue dans la décomposition du système dépend des données de SdF disponibles.
- Le modèle qualitatif contient implicitement des aspects quantitatifs (exp : le choix des modes de défaillance pour un composant est souvent de nature probabiliste. En effet, on ne retient que ceux connus sur la base d'une certaine expérience d'exploitation).
- L'analyse quantitative peut mettre en évidence certains aspects du système, qui nécessitent une analyse plus fine, remettant en cause la décomposition du système initialement retenue.

IV. 1. Itération : le processus d'une analyse de SdF est itératif. La SdF du système est fonction des objectifs fixés au début, et la configuration et/ou les modifications sur le système sont évaluées au regard de ces objectifs. L'analyse prendra fin une fois que les objectifs seront remplis.