République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département de Génie Electrotechnique et Automatique

Domaine: Sciences et Technologie
Filière: Automatique et informatique industriel
Spécialité: Commande et diagnostique des systèmes industriels

Projet de fin d'études

pour l'obtention du diplôme de Master Académique

Etude de la sûreté de fonctionnement des systèmes instrumentés de sécurité
Cas d'application : Drone de surveillance HERCULES 5 UF

Présenté par :

- BELAHCENE Houcem eddine
- MEJDOUB Abdallah

Sous la direction de :
Mme. BOUCEREDJ LEILA

Juin 2017

REMERCIEMENT

Je remercie DIEU tout puissant de m'avoir donné le courage et la patience pour réaliser ce travail.

Ce n'est pas la rédaction d'un tel rapport qui exige un remerciement, mais si on remercie des gens c'est par ce qu'ils méritent.

Au terme de ce travail, on tient à remercier Mdm. BOUCEREDJ Leila de nous avoir encadrés et suivis durant notre projet de fin d'étude. Ainsi qu'à tous les professeurs de l'université de Guelma, qui nous ont enseignés durant notre formation universitaire.

On remercie également nos parents pour leur soutien moral et financier durant nos études.

A tous nos collègues, amis, et tous ceux qui nous ont aidé et soutenu de près ou de loin.

DEDICACE

A mes chers parents

Pour leur soutien, leur patience, et leur sacrifice, vous méritez tout éloge,

J'espère être l'image que vous êtes fait de moi,

que dieu vous garde et vous bénisse.

Je dédie aussi ce travail à toute ma famille

A tous mes amis à l'Université de Guelma et ailleurs.

A tous ceux qui m'ont aidé.

Table des matières

Chapitre 2 : Les Systèmes Instrumentés de Sécurité

Chapitre 3 : Les méthodes d'analyse de la sûreté de fonctionnement

Chapitre 4 : Cas d'application : Drone de surveillance HERCULES 5 UF

Liste des Figures

Liste des tableaux

Introduction générale

Introduction générale

Les industries s'occupent non seulement des performances des systèmes en termes de qualité et de production mais aussi en termes de sûreté de fonctionnement et de sécurité. Les moyens à mettre en œuvre pour réduire les risques sont nombreux et varies. La conception du procédé, le choix des équipements participent à la réduction du risque. On peut aussi agir sur le système de contrôle commande du procédé, en prévoyant par exemple des redondances et des solutions de repli en cas des conditions anormales de fonctionnement. Ces approches ne sont pas toujours suffisantes.

Des systèmes spécifiques appelés Systèmes Instrumentés de Sécurité (SIS) sont utilisés ayant pour objectif de réduire les risques d'occurrence d'événements dangereux tout en garantissant la protection ; des personnes, des équipements matériels et de l'environnement.

Les SIS sont utilisés pour exécuter des fonctions de sécurité, ils sont aussi appelés boucles de sécurité. Ils comprennent les matériels et logiciels nécessaires pour obtenir la fonction de sécurité désirée pour traiter la sécurité fonctionnelle des systèmes. Les SIS ont pour objectif de mettre le procédé qu'ils surveillent en position de repli de sécurité lorsqu'il évolue vers une voie comportant un risque réel (explosion, feu, ...), c'est-à-dire dans un état stable ne présentant pas de risque pour les opérateurs humains et équipements.

La performance des SIS doit être prouvée par l'utilisation des analyses des méthodes de la sûreté de fonctionnement. Différentes méthodes sont citées dans ce mémoire parmi les méthodes citées, on trouve les blocs diagrammes de fiabilité, les arbres de défaillances, les réseaux de Pétri ainsi que les Graphe de Markov, ... On a choisi la méthode de l'AMDE pour analyser les différents modes de défaillance du système étudie, ensuite on a choisi le modèle RdPS couplé par des lois de fiabilité pour la recherche des scénarios redoutés, cela permet de déterminé la fiabilité des composant du système étudier pour déterminer la cause principale de la défaillance du système étudié.

Ce mémoire est composé de quatre chapitres. Nous introduirons dans le premier chapitre quelques notions relatives à la sûreté de fonctionnement. Nous introduisons la notion de SdF et quelques concepts généraux associés. Nous décrivons les principaux mécanismes de défaillance et les lois de fiabilité associées pour les différents types de composant.

Le deuxième chapitre est dédié aux systèmes instrumentés de sécurité (SIS). Un tour d'horizon est effectué décrivant les normes de sécurité relatives aux SIS. La norme CEI 61508 est la

3. Définition de la SdF :

La **sûreté de fonctionnement** est l'aptitude d'un système à remplir une ou plusieurs fonctions requises dans des conditions données ; elle englobe principalement quatre composantes : la fiabilité, la maintenabilité, la disponibilité et la sécurité. La connaissance de cette aptitude à remplir une ou plusieurs fonctions permet aux utilisateurs du système de placer une confiance justifiée dans le service qu'il leur assure. Par extension, la sûreté de fonctionnement désigne également l'étude de cette aptitude et peut ainsi être considérée comme la « science des défaillances et des pannes » [2].

Selon [3], la SdF est la propriété d'un système permettant à ses utilisateurs de placer une confiance justifiée dans le service délivré.

Elle peut être caractérisée par les attributs suivants :

a) La ***fiabilité*** : c'est l'aptitude d'une entité à accomplir une fonction requise, dans des conditions données, pendant une durée donnée. Elle est généralement mesurée par la probabilité qu'une entité accomplisse une fonction requise, dans les conditions données, pendant l'intervalle de temps [0, t].

MESURE : Probabilité qu'un système S accomplisse une fonction requise, dans des conditions données, pendant l'intervalle de temps (0, t).

R(t) = P [S non défaillant sur (0, t)]

Ex: $$\boldsymbol{P = \lambda e^{-\lambda t}\ (\lambda\ constant)}$$

La propriété de fiabilité est sans doute la propriété la plus recherchée puisqu'elle concerne l'aptitude d'un système à fournir de façon continue un service correct. En général, elle est mesurée par la probabilité de ne pas tomber en panne jusqu'à une date t. Elle permet également d'estimer quantitativement le temps moyen de fonctionnement correct avant la défaillance (en anglais, Mean Time To Failure ou MTTF).

b) La ***disponibilité*** : c'est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données et à un instant donné. La disponibilité est généralement mesurée par la probabilité qu'une entité soit en état d'accomplir une fonction requise dans des conditions données et à un instant t donné.

MESURE : Probabilité qu'un système S soit en état d'accomplir une fonction requise dans des conditions données et à un instant donné.

D(t) = P [S non défaillant à l'instant t]

Cet attribut de la SdF est généralement mesuré par la probabilité de fonctionner correctement à l'instant t. Dans le cas d'un système réparable, il permet d'exprimer la proportion de temps où le service est correct avant défaillance par rapport au temps moyen entre deux défaillances :

Disponibilité = A = MTTF/(MTTF + MTTR) = MTTF/MTBF

Avec MTTR signifiant temps moyen de réparation (en anglais, Mean Time To Repair) et MTBF temps moyen entre deux défaillances (en anglais, Mean Time Between Failure).

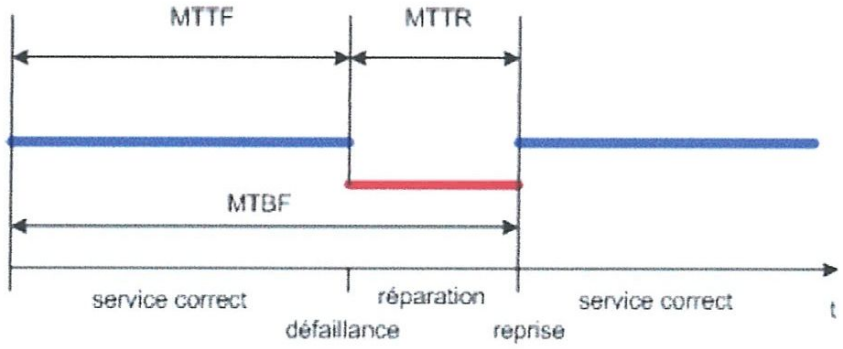

Figure 1.1 : Estimation de la fiabilité et de la disponibilité.

c) La ***maintenabilité*** : c'est l'aptitude d'une entité à être maintenue ou rétablie dans un état dans lequel elle peut accomplir une fonction requise, lorsque la maintenance est effectuée dans des conditions données avec des procédures et des moyens prescrits. Elle est généralement mesurée par la probabilité que la maintenance d'une entité accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t, sachant que l'entité est défaillante à l'instant t = 0.

MESURE : Probabilité que la maintenance d'un système S accomplie dans des conditions données, avec des procédures et des moyens prescrits, soit achevée au temps t, sachant que le système est défaillant à t = 0.

M(t) = P [S est réparé sur (0, t)]

La compréhension des termes utilisés en maintenabilité rend nécessaire l'établissement d'un diagramme chronologique des temps entre l'instant de l'apparition de la défaillance et l'instant de la remise en service de l'installation. Le diagramme de la (***figure 1.2***) résume tous les instants importants de cette chronologie.

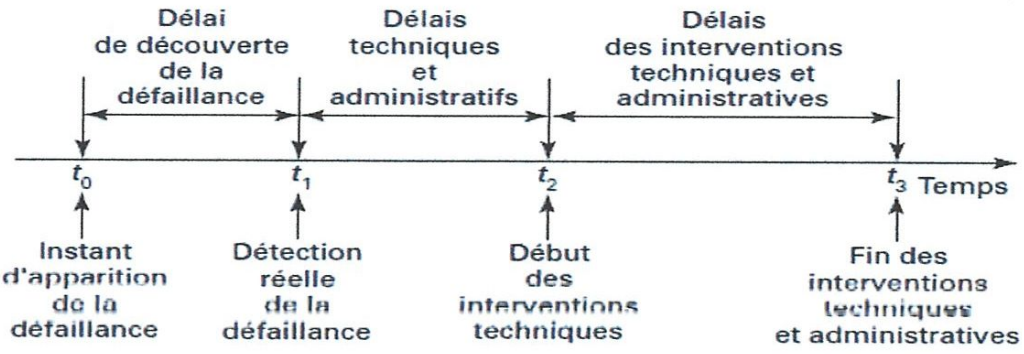

Figure 1.2 : Chronologie des temps des activités de maintenance

Dans cette séquence, l'instant t0 correspond à l'instant de l'apparition réelle de la défaillance. En fonction des moyens mis à la disposition des opérateurs (systèmes d'alarme ou bien informations venant de rondes de surveillance), il s'écoulera un délai t1 – t0 allant de quelques secondes à quelques heures pour réaliser le diagnostic de la présence d'une défaillance. La confirmation de la défaillance ayant été réalisée, il s'écoule des délais techniques et administratifs pour réunir les personnels, les pièces détachées et les autorisations administratives (par exemple, consignation d'autres matériels) pour débuter les opérations de réparation. A partir du temps t2, les opérations de maintenance peuvent se dérouler et incluent également les procédures d'assurance qualité et l'obtention des autorisations administratives éventuelles (par exemple, pour les appareils à pression soumis à réglementation). Ce n'est qu'à partir du temps t3 que l'on peut considérer que l'installation est devenue à nouveau opérationnelle.

La (***figure 1.3***) représente l'allure de la maintenabilité M (t) en fonction du temps.

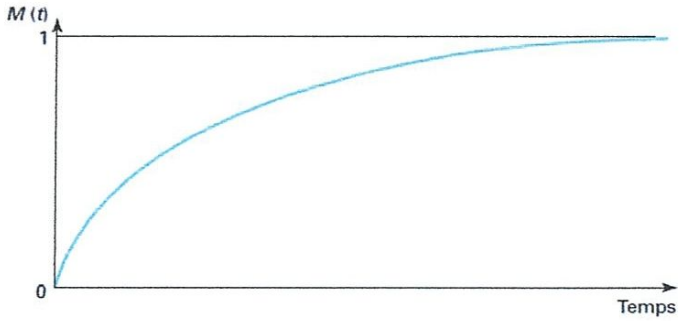

Figure 1.3 : Allure de la courbe de maintenabilité

On constate qu'à l'origine des temps M (0) = 0, ce qui est évident car l'entité est défaillante. Elle possède une asymptote égale à 1 car l'on peut supposer qu'elle sera réparée au bout d'un temps donné sinon cette entité ne serait d'aucune utilité.

La maintenabilité d'une entité dépend étroitement des moyens et compétences mis en œuvre. Comme pour la fiabilité, la notion de maintenabilité dépend de l'état initial de l'entité étudiée. Au plan pratique, la comparaison des performances d'entités identiques n'a de sens que si les méthodes et outils de maintenance sont appliqués dans des conditions strictement identiques.

- ***Taux de réparation***

On appelle taux de réparation μ (t) d'un système réparable au temps t la probabilité que l'entité soit réparée entre t et t + dt sachant qu'elle n'était pas réparée sur l'intervalle [0, t].

Elle se note : μ (t) = P (entité réparée sur [t, t + dt] sachant qu'elle n'était pas réparée sur [0, t]).

- ***MTTR***

Le terme MTTR (mean time to repair) est la durée moyenne jusqu'à la réparation d'une entité réparable. Pour cette variable aléatoire, le MTTR se calcule par la formule :

$$MTTR = \int_0^{+\infty} \big(1 - M(t)\big)dt$$

Le MTTR s'assimile ainsi à la durée moyenne jusqu'à la première réparation et requiert la connaissance de l'état initial de l'entité.

Comme il y a en général plusieurs modes de défaillances, il faut définir plusieurs MTTR d'une entité : à chaque mode de défaillance correspondra un MTTR spécifique.

Cela implique de définir clairement le ou les états de l'entité pour lesquels celle-ci est considérée comme réparée.

➢ ***Relation entre F, M et D :***

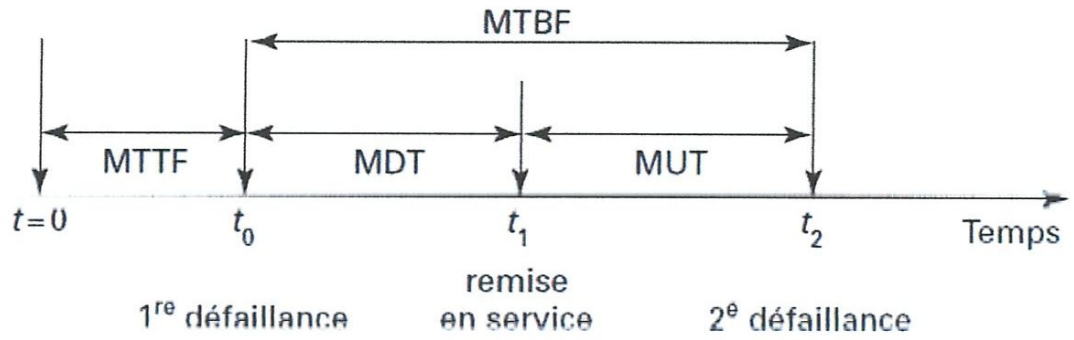

Figure 1.4 : Relations entre les liens temporels en fiabilité, disponibilité et maintenabilité

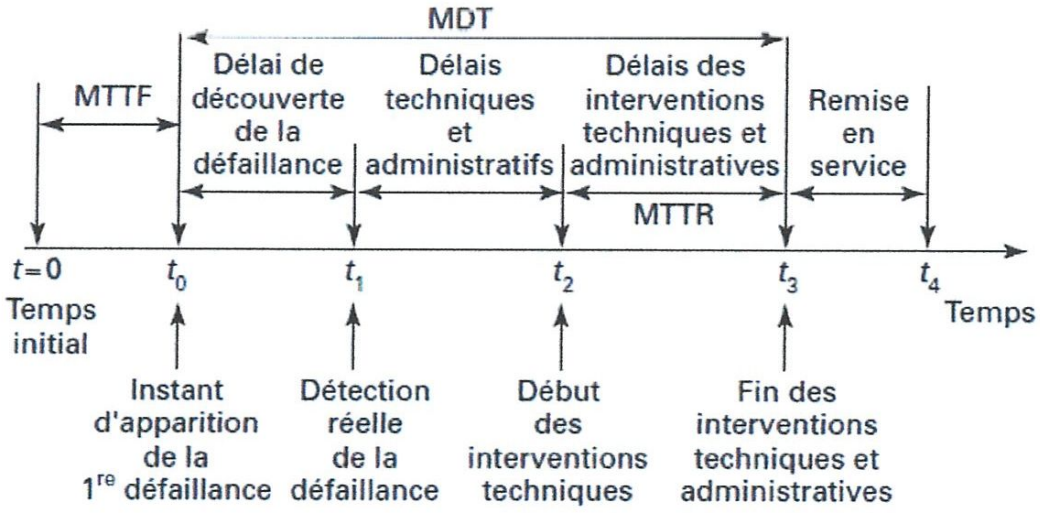

Figure 1.5 : Chaînage temporel des activités de détection et de remise en service

Les ***(figures 1.4*** et ***1.5***) récapitulent les liens temporels entre les différents termes définis en fiabilité, disponibilité et maintenabilité.

d) La ***sécurité*** : c'est l'aptitude d'une entité à éviter de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques. La sécurité est

généralement mesurée par la probabilité qu'une entité évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

> *MESURE* : Probabilité qu'un système S évite de faire apparaître, dans des conditions données, des événements critiques ou catastrophiques.

La sécurité restant un terme très général, il n'existe pas actuellement de consensus pour une normalisation. La terminologie en usage en France ne fait pas la différence entre les termes anglais « security » et « safety ».

L'évaluation de la sécurité est actuellement encore limitée et est effectuée pour les installations chimiques, les centrales nucléaires, les plates-formes pétrolières et l'aéronautique. Elle est basée sur des études statistiques des impacts des accidents (réels, expérimentés ou simulés) sur l'homme et l'environnement (notion de gravité).

Le développement d'un système sûr de fonctionnement passe par l'utilisation combinée d'un ensemble de méthodes, appelées moyens de la sûreté de fonctionnement, qui peuvent être classées en :

- Prévention des fautes, comment empêcher par construction, l'occurrence ou l'introduction de fautes
- Tolérance aux fautes, comment fournir par redondance, un service conforme à la spécification en dépit des fautes,
- Elimination des fautes, comment minimiser par vérification la présence de fautes,
- Prévision des fautes, comment estimer la présence, la création et les conséquences de fautes.

La Sûreté de Fonctionnement a pour objectif de spécifier, concevoir, réaliser et exploiter des systèmes où la faute est naturelle, prévue et tolérable [3].

La maîtrise des risques représente une discipline à part entière et fait l'objet d'ouvrages spécialisés et de techniques spécifiques des industries concernées (transport, chimie, nucléaire...).

La (***figure 1.6***) résume les liens entre fiabilité, maintenabilité, disponibilité et sécurité.

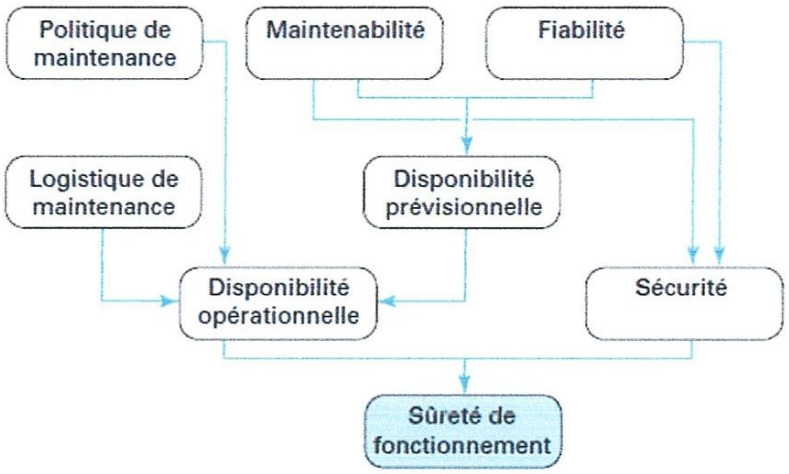

Figure 1.6 : Relations entre fiabilité, maintenabilité, disponibilité et sécurité

Le schéma complet de la taxonomie de la sûreté de fonctionnement est donné à la figure A.1 :

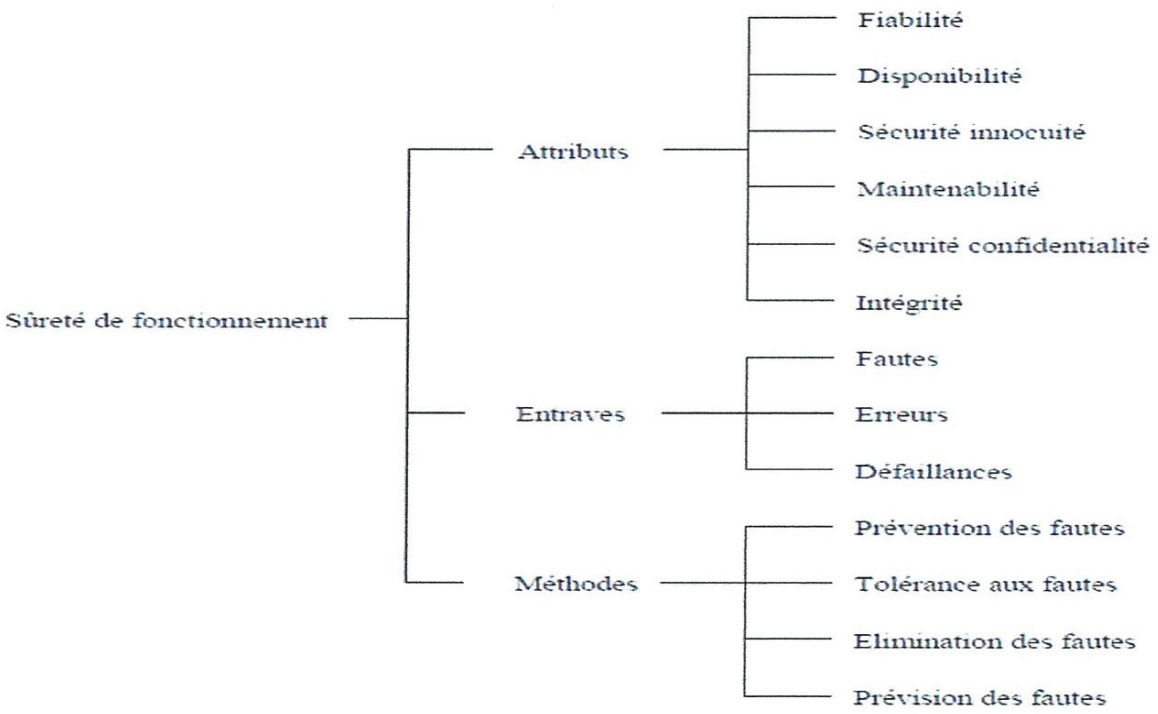

Figure 1.7 : Taxonomie de la sûreté de fonctionnement [4]

4. Entraves à la sûreté de fonctionnement

Les entraves de la sûreté de fonctionnement : fautes, erreurs et défaillances sont les circonstances indésirables, causes ou résultats de la non sûreté de fonctionnement.

Une défaillance du système survient lorsque le service délivré dévie de l'accomplissement de la fonction du système, c'est-à-dire de ce à quoi le système est destiné. Une erreur est la partie de l'état du système qui est susceptible d'entraîner une défaillance, c'est-à-dire qu'une défaillance se produit lorsque l'erreur atteint l'interface du service fourni, et le modifie. Une faute est la cause adjugée ou supposée d'une erreur. Il existe donc une chaîne causale entre faute, erreur et défaillance.

4.1 Défaillance :

Une défaillance est la cessation de l'aptitude d'une entité à accomplir une fonction requise. La défaillance d'une entité résulte de causes qui peuvent dépendre des circonstances liées à la conception, la fabrication ou l'emploi et qui ont entrainé la défaillance. Enfin, le mode de défaillance est l'effet par lequel une défaillance est observée (définition de la Commission Electrotechnique Internationale).

Le service délivré étant une séquence d'états externes, une défaillance du service signifie qu'au moins un état externe dévie du service correct. La déviation est une erreur. La cause adjugée ou supposée d'une erreur est une faute. Les fautes peuvent être internes ou externes au système. La présence antérieure d'une vulnérabilité, c'est-à-dire d'une faute interne qui permet à une faute externe de causer des dommages au système, est nécessaire pour qu'une faute externe entraîne une erreur et, éventuellement, une défaillance.

4.2 Cause de défaillance :

Généralement, une faute cause d'abord une erreur dans l'état interne d'un composant, l'état externe du système n'étant pas immédiatement affecté. Il s'ensuit la définition d'une erreur : partie de l'état total du système qui est susceptible d'entraîner sa défaillance, qui survient lorsque l'erreur affecte le service délivré à l'utilisateur. Il est à noter que nombre d'erreurs n'affectent pas l'état externe du système, et donc ne causent pas de défaillance.

La spécification de sûreté de fonctionnement d'un système décrit ce qui est requis pour les attributs de la sûreté de fonctionnement en termes de fréquence et de gravité des défaillances du service pour un ensemble donné de fautes, pour un environnement opérationnel donné. Ainsi, il s'ensuit une définition alternative de la sûreté de fonctionnement, donnée au début de ce chapitre, et qui complète la définition initiale en procurant un critère pour décider si la confiance dans le service peut être placée ou non : aptitude à éviter des défaillances du service plus fréquentes ou plus graves que l'acceptable.

Des défaillances du service plus fréquentes ou plus graves que ce qui est acceptable manifestent une défaillance de la sûreté de fonctionnement.

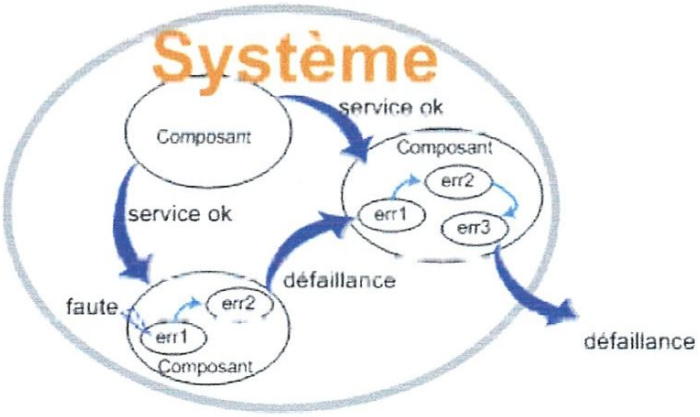

Figure 1.8 : Propagation d'un dysfonctionnement.

Ainsi, nous pouvons résumer ces définitions en ces quelques mots : une erreur est un état susceptible d'entraîner une défaillance ; cette erreur peut être latente comme elle peut être détectée ; la propagation d'une erreur peut produire d'autres erreurs ; une faute est une cause adjugée ou supposée d'une erreur ; une défaillance est une manifestation d'une erreur qui par propagation traverse la frontière du système avec son environnement. Nous pouvons ainsi schématiser la relation entre ces entraves par la figure suivante :

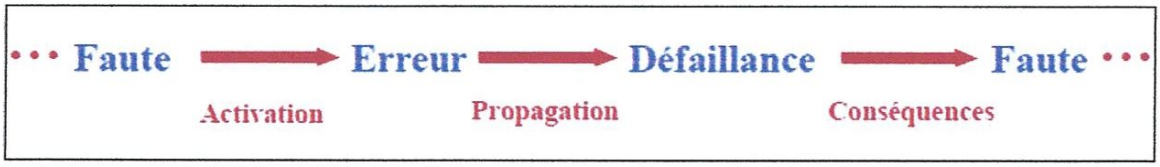

Figure 1.9: La chaîne fondamentale des entraves à la sûreté de fonctionnement

Les flèches de cette chaîne expriment la relation causale entre fautes, erreurs et défaillances. Elles doivent être interprétées de façon générique : par propagation, plusieurs erreurs sont généralement générées avant qu'une défaillance ne survienne.

5. Les lois de la SdF

5.1 Taux de défaillance :

Généralement noté λ(t), est

$$\lambda(t) = \frac{-\frac{dR(t)}{dt}}{R(t)}$$

Il représente l'intensité de défaillance de fonction du temps. C'est la probabilité conditionnelle, divisée par *dt,* de tomber en panne entre *t* et *t+dt* sachant qu'au temps *t* l'entité n'est pas défaillante.

L'hypothèse est très souvent faite que ce taux de défaillance est constant (indépendant du temps). Alors la loi de fiabilité prend une forme facile à manipuler de :

$$R(t) = exp(-\lambda t)$$

En fait, cette hypothèse très pratique est assez audacieuse, mais l'expérience a montré que, pour des nombreuses catégories de composants, il y avait une période assez longue entre la jeunesse et la vieillesse pendant laquelle cette hypothèse était une approximation tout à fait acceptable (encore faut-il vérifier qu'on exploitera effectivement cette seule période de la vie des composants si on a pris cette hypothèse pour les calculs prévisionnels). On constate souvent que la courbe représentant le taux de défaillance d'une série de composants en fonction du temps à la forme dite « courbe baignoire » :

- La décroissance rapide de la fréquence des défaillances correspondant au « déverminage » et à l'élimination des défauts de jeunesse ;
- Le fond de la baignoire correspondant à la période de maturité ou le taux de fiabilité des composants est le meilleur et, souvent, à peu près constant ;
- En fin, la remontée progressive de la fréquence des défaillances correspond à la vieillesse

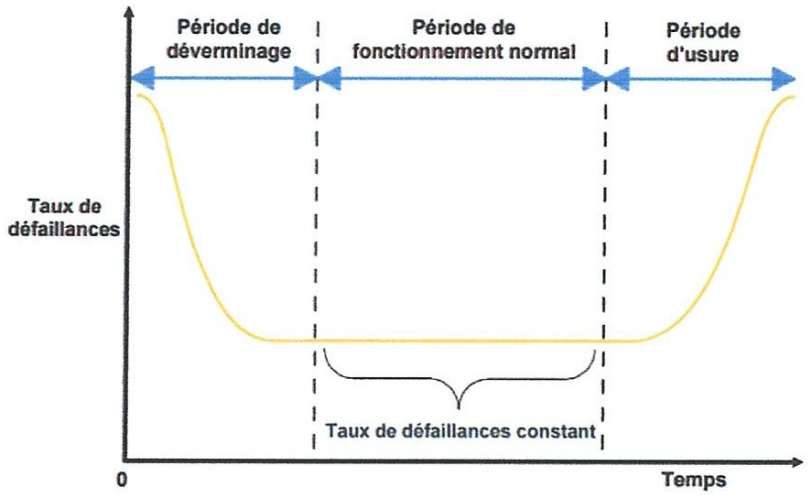

Figure 1.10 : Evolution du taux de panne avec le temps

5.1.1 Les composants mécaniques

Les composants mécaniques sont soumis, dès le début de leur vie, au phénomène d'usure ou de vieillissement. Si on trace la courbe du taux de défaillance, en fonction du temps, on obtient une courbe qui ne présente pas le plateau de la (***Figure 1.10***) ; la période de vie utile (taux de défaillance constant) n'existe pas ou elle est réduite.

- La première phase définit la période de mortalité infantile. C'est une durée de vie en principe très courte. Elle est décrite par une décroissance progressive du taux de défaillance avec le temps dû à une amélioration des caractéristiques internes (caractéristiques de défauts) et des interfaces, par un rodage préalable des pièces. Parmi les distributions de probabilité pour ces conditions, la loi de Weibull ($\beta < 1$) et loi lognormale ($\sigma > 1$) sont les plus utilisées.
- La dernière phase définit la période de vieillissement qui recouvre la majeure partie de la vie du dispositif. Elle est caractérisée par une augmentation progressive du taux de défaillance. Les pièces mécaniques sont soumises à des phénomènes de vieillissement multiples qui peuvent agir en combinaison : corrosion, usure, fluage, fatigue, et finalement rupture. Les distributions de probabilité utilisées pour ces conditions sont la loi de Weibull ($\beta > 1$) et la loi lognormale ($\sigma < 1$).

Les composants mécaniques sont caractérisés par des mécanismes de dégradation souvent complexes, d'origines variées (fatigue, fluage, fissuration, usure, corrosion/oxydation, désagrégation)

La **fatigue** consiste dans la dégradation ou la modification des propriétés mécaniques des matériaux, suite à l'application répétée d'un chargement cyclique ou d'une vibration, conduisant à une rupture. La fatigue est la plus importante source de défaillance pour les composants mécaniques comme, par exemple, les roulements à billes.

Le **fluage** est un mécanisme de dégradation lié au chargement et à la température conduisant à une déformation du matériau (allongement ou élongation). Ce mécanisme devient prépondérant dès que la température du matériau dépasse une certaine valeur (environ 400°C pour les aciers).

L'usure est liée au frottement entre deux pièces mécaniques provoquant l'augmentation du jeu entre elles (élimination de matière). Ex : les pneus, les roulements.

La plupart des métaux sont détériorés par l'interaction avec l'oxygène (la **corrosion** ou **l'oxydation**).

Ces modes de dégradation font intervenir plusieurs paramètres :

- Les caractéristiques matériaux (limite élastique, limite à la rupture, limite d'endurance, limite de fatigue, ténacité, dureté,),
- Les caractéristiques dimensionnelles (géométrie,),
- Les sollicitations extérieures (température, chargement, pression, ...).
- La forte interaction entre le composant et son environnement (contrainte chimique comme l'oxydation, vibration,)

5.1.2 Les composants électroniques

Pour les composants électroniques la courbe, représentant le taux de défaillance, a la même allure que la courbe en baignoire (***Figure 1.10***). Elle est donc composée de trois phases nettement distinctes :

- La première phase définit la période de jeunesse, caractérisée par une décroissance rapide du taux de défaillance. Pour un composant électronique cette décroissance s'explique par l'élimination progressive des défauts dus aux processus de conception ou de fabrication mal maîtrisé ou à un lot de composants défectueux. Aujourd'hui, cette période est réduite, compte tenu de la grande qualité des composants. Les distributions de probabilité utilisées pour ces conditions sont la loi de Weibull ($\beta < 1$) et la loi lognormale ($\sigma > 1$).
- La deuxième phase définit la période de vie utile généralement très longue. Le taux de défaillance est approximativement constant. Les pannes sont dites aléatoires, leur apparition n'est pas liée à l'âge du composant mais à d'autres mécanismes

d'endommagement. Le choix de la loi exponentielle est tout à fait satisfaisant dans cette phase.

– La dernière phase est la période de vieillissement, elle est caractérisée par une augmentation progressive du taux de défaillance avec l'âge du système. Cette augmentation est due aux phénomènes de vieillissement tels que l'usure, l'érosion, etc. Cette période est très nettement au-delà de la durée de vie réelle d'un composant électronique. Les distributions de probabilité utilisées pour ces conditions sont la loi de Weibull ($\beta > 1$) et la loi lognormale ($\sigma < 1$).

Les composants électroniques présentent des mécanismes de dégradation complexes telles que les charges de surface, la polarisation, le décollement de fils de connexion, la migration métallique, l'électromigration, le défaut de silicium, ...

- Les **charges de surface** représentent la présence de charges en surface des oxydes de grille. Ce mécanisme intervient dans la dérive de la tension de seuil.
- La **polarisation** suppose la présence de molécules polarisables dans l'oxyde de grille. Elle entraîne la dérive de la tension de seuil.
- Le **décollement de fils de connexion** est lié directement au processus d'assemblage et provoque souvent des courts-circuits.
- La **migration métallique** est le déplacement des atomes du métal dans le silicium et entraîne des courts-circuits ou des circuits ouverts.
- **L'électromigration** représente le déplacement des atomes dans les couches métalliques et provoque des courts-circuits.
- Un **défaut de silicium** est provoqué par des impuretés, des défauts de structure ou bien par des états de surface et entraîne des courts-circuits.

Ces modes de défaillances agissent principalement sur les caractéristiques suivantes du composant :

– la tension de seuil (dérive provoquée par surcharge, perte ou inversion de charge, polarisation, ...),

– les circuits (ouverture/fermeture par impureté, défaut de structure dans le matériel, oxydation, ...).

5.1.3 Les composants logiciels

La courbe en baignoire ne s'applique pas strictement au logiciel. Cependant, le cycle de développement du logiciel peut être comparé avec le cycle de vie du matériel. Ainsi, pendant la période du cycle de développement, le taux de défaillance logiciel est caractérisé par la courbe en baignoire.

La première phase commence avec les tests et est considérée comme la phase de correction. Les erreurs de programmation ou les opérations non conformes aux spécifications sont identifiées et corrigées

La deuxième phase représente la période de vie utile du logiciel dans laquelle le taux de défaillance est constant. La distribution utilisée lors de cette phase est la loi exponentielle

La dernière phase commence à la fin de la vie utile. La plupart des erreurs observées pendant cette période sont dues à l'incapacité du logiciel à satisfaire des nouveaux besoins du client, sans modification des spécifications initiales. Nous pouvons considérer ce phénomène comme l'"usure" du logiciel. Les "défauts" observés pendant cette période peuvent servir comme base pour un nouveau logiciel. En plus, il y a le phénomène de vieillissement du logiciel, comme notamment les problèmes liés aux systèmes d'exploitation.

Les composants logiciels sont caractérisés par une typologie particulière de dégradation (Défaillance, erreur, faute). [3] Notons que pour les composants logiciels il existe une chaîne causale entre la faute, l'erreur et la défaillance.

La **défaillance** est l'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.

L'erreur est la partie de l'état du système qui est susceptible d'entraîner une défaillance.

La **faute** est la cause adjugée ou supposée d'une erreur.

Ces modes de dégradation agissent principalement sur les caractéristiques suivantes :

– La valeur de l'information délivrée (accomplissement de la fonction du composant logiciel),

– Le service délivré (correctitude, cohérence perçue par tous les systèmes/utilisateurs, conséquence vis-à-vis d'autres systèmes/environnement).

Les différentes technologies sont caractérisées par des mécanismes de défaillance distincts, décrits par des lois de distribution de probabilité.

5.2 Notion de temps MTBF, MTTR, MTTF, MUT, MDT :

A l'origine des confusions, il y a un jeu des mots : en anglo-américain, on utilise les sigles MTTF (Mean Time To Failure) et MTBF (Mean Time Between Failure). Ce dernier sigle peut donc se transposer directement en français en MTBF (Moyenne Des Temps de Bon Fonctionnement), mais pas avec la même signification.

a) **MTTF** (*Mean Time To Failure*) **:** Durée moyenne de fonctionnement avant défaillance, espérance mathématique de la durée de fonctionnement avant défaillance. La définition du MTTF est :

$$MTTF = \int_0^\infty R(t)dt$$

Le MTTF est la moyenne des durées de fonctionnement de l'instant 0 à la première défaillance

b) **MTBF** (*Mean Time Between Failures*) : Est la moyenne des temps séparant deux défaillances consécutives.

Pour une entité réparable, connaissant une alternance de périodes de fonctionnement ininterrompu et de périodes de remise en état de fonctionnement, le MTBF est la moyenne de durées dont chacune est constituée d'une période de remise en état après défaillance suivie d'une période de fonctionnement ininterrompu.

$$MTBF = \frac{1}{\lambda}$$

c) **MTTR** (*Mean Time To Repair or restoration*) : durée moyenne de panne ou moyenne des temps pour la remise en état de fonctionnement, espérance mathématique de la durée de panne. MTTRep est associé à la réparation du composant et MTTRes à sa restauration. La différence entre les deux est liée au fait que l'on considère ou non le temps mis pour remettre en service l'équipement, le MTTRes l'incluant.

d) **MUT** (*Mean Up Time*) **:** La moyenne des temps de fonctionnement.

En générale, un système satisfaisant connaît des périodes de panne beaucoup plus courtes que les périodes de bon fonctionnement ininterrompu ; de ce fait, le MTBF est à peine plus élevé que le MUT et la confusion entre les deux peu importante. Parmi les erreurs d'interprétation les plus courantes touchant le MTBF, il y a celle qui consiste à croire que le MTBF est le temps pendant lequel on peut espérer être épargné par les défaillances. Pour illustrer le danger de ce type d'interprétation, considérons le cas très usuel où l'hypothèse du taux de défaillance constant est retenue.

e) **MDT** (*Mean Down Time*) : ou TMI temps moyen d'indisponibilité, espérance mathématique de la durée d'indisponibilité.

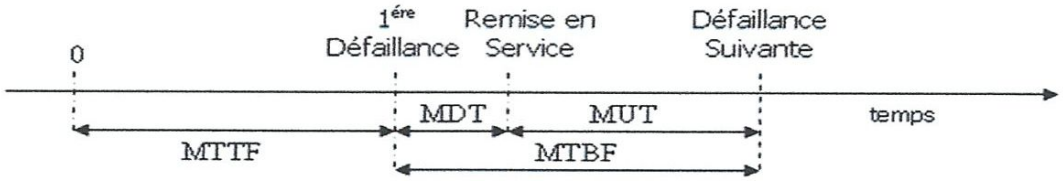

Figure 1.11 : Moyennes temporelles caractéristiques

5.3 Principales lois rencontrées dans l'étude de fiabilité :

Nous présentons quelques propriétés des principales lois utilisées en sureté de fonctionnement ; on distingue :

5.3.1 Lois discrètes :

a) Loi binominale :

Elle correspondant à la probabilité de réalisation d'un évènement de probabilité P au cours de (n) expériences.

La variable aléatoire discrète est distribuée suivant une loi binominale de paramètre (P,n) telle que

$$P(X = i) = C_n^i . P^i . (1 - P)^{(n-1)} \; ; 0 \leq i \leq n \; et \; 0 \leq p \leq 1$$

On en déduit la fonction de répartition :

$$F(i) = P(x \leq i) = \sum_{i=0}^{i} C_n^i . Pi . (1 - P)^{(n-1)}$$

La valeur moyenne est la variance sont données par :

$$m = E[X] = n.p \; et \; \sigma^2[X] = n.p(1 - p)$$

b) ***Loi de poisson :***

Elle correspond au nombre d'occurrences sur une période donnée d'un évènement dans la probabilité par unité de temps est constant. La loi de poisson est une loi à un paramètre positive (m) définie par :

$$p(X = K) = e^{-m} . \frac{m^k}{k!}$$

On déduit la fonction de répartition :

$$F(k) = \sum_{i=0}^{k} e^{-m} . \frac{m^k}{k!} \; ou \; E[X] = m \; et \; \sigma^2[X] = m$$

5.3.2 Lois continues :

a) ***Loi exponentielle :***

La loi exponentielle est très fréquemment utilisée en fiabilité car elle est des seules qui permettent de réaliser les calculs. Le taux de défaillance d'un élément dont la distribution des temps de bon fonctionnement est une loi exponentielle, et constant et égale à λ.

La variance aléatoire dans ce cas est une variable continue, t entre [0 , +∞[dont la densité de probabilité est donnée par : $\boldsymbol{f(t) = \lambda e^{(-\lambda t)}}$

La moyenne et la variance sont données par : $\boldsymbol{m = 1/\lambda}$ *et* $\boldsymbol{\sigma^2[X] = 1/\lambda}$

Avec les paramètres de significations :

e : est la base de l'exponentielle (2,718...)

λ : c'est l'intensité.

Les distributions relatives à cette loi sont représentées par les courbes de la figure en fonction du taux de défaillance d'un ou plusieurs composants supposés avoir un même λ.

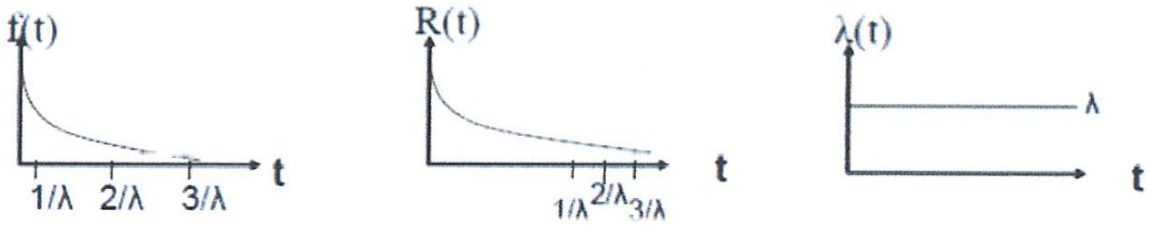

Figure 1.12 : distribution des fonctions de la loi exponentielle

La distribution exponentielle s'applique aux systèmes opérants en continu (systèmes électroniques) c'est ce qu'on appelle distribution sans mémoire. Les systèmes complexes ont aussi un λ(t) constant.

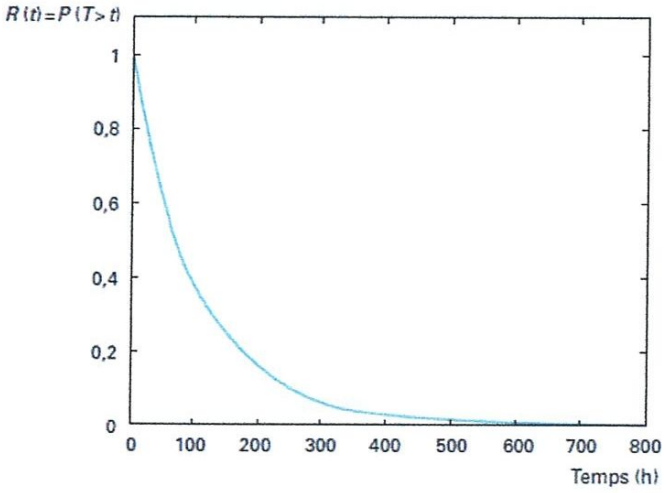

Figure 1.13 : Allure de la fonction R (t) pour la loi exponentielle

La figure 7 représente une allure de la fiabilité R (t) en fonction du temps pour une loi exponentielle définie par : $R(t) = \exp(-\lambda t)$

Avec : $t > 0$ et $\lambda > 0$

b) ***Loi de Galton :***

Une autre distribution couramment utilisé est la loi de Galton, elle a été introduite pour la modélisation des durées de vie des semi-conducteurs à partir de constatation statistique. Son champ d'application touchant déjà de nombreux domaines, depuis l'économie jusqu'à la cancérologie.

La variable aléatoire dans ce cas est une variable continue, t entre $[0 \ +\infty[$ dont la densité de probabilité est donnée par :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \cdot \frac{1}{t} \cdot exp\left\{-\frac{1}{2}\left(\frac{ln(t) - m'}{\sigma'}\right)^2\right\}$$

Avec m': moyenne des ***ln(t)***

σ' : écart – type des ***ln(t)***

La valeur moyenne et la variance sont données par :

$$m = exp\left(m + \frac{\sigma^2}{2}\right) \ et \ \sigma^2(t) = \frac{1}{\lambda^2}$$

c) Loi normale (loi de gauss) :

Cette loi est symétrique par rapport à la moyenne m. La variance aléatoire est dans ce cas une variable continue t entre $]-\infty \ +\infty[$ dont la loi de densité de probabilité est donnée par :

$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} \cdot exp\left\{-\frac{1}{2}\left(\frac{t-m'}{\sigma'}\right)^2\right\}$$

La valeur moyenne et la variance sont données par :

$$m = m' \ \ et \ \ \sigma^2(t) = \sigma'^2$$

d) Loi uniforme :

La variable aléatoire t est, dans ce cas, une variable continue dans $[t_1,t_2]$ dont la loi de densité de probabilité est donnée par :

$$f(t) = \frac{1}{t_2 - t_1}$$

La valeur moyenne et la variance sont données par :

$$m = \frac{t_2 + t_1}{2} \quad et \quad \sigma^2 = \frac{(t_2 + t_1)^2}{12}$$

e) Loi de weibull :

Voici maintenant, la plus populaire des lois rencontrées en fiabilité aussi bien dans les domaines mécaniques qu'électronique. Cette loi est très utilisée pour représenter le comportement des matériels pendant toute leur période de vie avec une loi de densité de probabilité définie par :

$$f(t) = \frac{\beta(t-\gamma)^{\beta-1}}{\eta^{\beta}} . exp - \left(\frac{t-\gamma}{\eta}\right)^{\beta}$$

Sa fonction de fiabilité est donnée par :

$$R(t) = exp - \left(\frac{t}{\eta}\right)^{\beta}$$

Le taux de défaillance est donné par :

$$\lambda(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1}$$

Avec :

β : paramètre de forme (sans unité).

η: paramètre d'échelle (en unité de temps).

γ: paramètre de position (en unité de temps).

La valeur moyenne et la variance sont données par :

$$m = \gamma + \eta.\Gamma\left(\frac{1+\beta}{\beta}\right) \quad et \quad \sigma^2(t) = \eta^2\left\{\Gamma\left(\frac{2}{\beta}+1\right) - \Gamma^2\left(\frac{1+\beta}{\beta}\right)\right\}$$

Avec :

$$\Gamma(b) = \int_0^{+\infty} x^{b-1}.exp(-x)dx$$

6. Conclusion :

La SdF traduit un besoin de confiance sur les systèmes développés. Cette confiance est apportée par de nombreuses méthodes et pratiques en cours qui associent des formalismes mathématiques à des connaissances a priori du comportement attendu. Des architectures dédiées à la SdF sont alors développées pour anticiper la gestion des défaillances auxquelles tout système artificiel est sujet.

Chapitre 2

Les systèmes instrumentés de sécurité

1. Introduction :

L'industrie de processus devient techniquement de plus en plus complexe et le potentiel de danger s'accroît en conséquence si les flux de danger ne sont pas convenablement contrôlés. Ainsi, lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont à mettre en œuvre. Celles-ci participent soit à la prévention en minimisant la probabilité d'apparition du risque, soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS) sont utilisés pour assurer la sécurité fonctionnelle des installations, la réduction des risques à un niveau inférieur ou égal au risque tolérable. Pour concevoir les SIS, deux normes de sécurité sont utilisées : l'IEC 61508 (IEC, 1998) et l'IEC 61511 (IEC, 2004).

Les normes ANSI/ISA 884.01-1996 et CEI 61511 établissent les prescriptions relatives à la spécification, la conception, l'installation, l'exploitation et la maintenance du SIS, afin d'avoir toute confiance dans sa capacité à amener le procédé dans un état sûr. Les étapes de base pour se conformer à ces normes sont :

- Etablir une cible de sécurité (risque acceptable) du procédé et évaluer le risque existant.
- Identifier les fonctions de sécurité requises et les affecter aux niveaux de protection.
- Déterminer si la fonction instrumentée de sécurité est requise.
- Implémenter la fonction instrumentée de sécurité dans un SIS et déterminer 1e SIL du SIS.
- Vérifier que le SIS permet d'atteindre 1a cible de sécurité exigée au départ.

Toute 1a difficulté est d'estimer 1e risque que présente 1e procédé et d'évaluer la diminution du risque que doit apporter 1e système instrumenté de sécurité. La nonne formalise une démarche :

- D'analyse de risque qui identifie ce qui doit être fait pour éviter les événements dangereux associés au procédé
- D'évaluation de risque permettant l'obtention de l'intégrité de la sécurité exigée du système pour que le risque devienne acceptable.

La mise en œuvre des prescriptions de ces deux normes est assez difficile et les méthodes proposées dans leurs annexes doivent être utilisées avec précaution [13]. Toutefois, un élément

clairement établi dans le processus de conception d'un SIS est qu'il doit aboutir à la satisfaction d'un niveau d'Intégrité de Sécurité (SIL) alloué [18]. Le SIL exprime ainsi la réduction de risque que doit apporter un SIS au système qu'il surveille. La contrainte d'une conception de SIS est donc de satisfaire au niveau de SIL requis tout en minimisant le coût de conception, d'exploitation ... Il s'agit donc d'un problème d'optimisation où le coût doit être minimisé sous des contraintes de performance de sureté de fonctionnement.

2. Système instrumenté de sécurité :

2.1. Définition :

Un **système instrumenté de sécurité** est un système visant à mettre un procédé en position de repli de sécurité (c'est-à-dire un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu...).

Les systèmes instrumentés de sécurité sont utilisés pour exécuter des fonctions de sécurité dans les industries de production par processus (ou de transformation). Ce sont des moyens de sécurité chargés de surveiller que le procédé ne franchit pas certaines limites (au-delà desquelles il pourrait devenir dangereux) et d'actionner les organes de sécurité lorsqu'un tel danger se présente.

Les SIS sont une composante essentielle des dispositifs de prévention des installations industrielles. La définition des fonctions de sécurité, la conception, la maintenance, et la modification des systèmes doivent assurer la disponibilité et la fiabilité de la fonction de sécurité en toute circonstance.

Un SIS se compose de trois parties :

- Une couche capteur (Sensor) : elle est constituée d'un ensemble d'éléments d'entrée (ex : capteurs, détecteurs) qui surveillent l'évolution des paramètres physicochimiques représentatifs du comportement du procédé (température, pression, niveau . . .).
- Une couche unité logique LS (Logic Solver) : ce sous-ensemble d'éléments logiques réalise le processus de prise de décision qui s'achève par l'activation du troisième sous-système FE (Final Element) [14]. Le sous-système LS peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques.

- Une couche actionneur FE : Elle agit directement (ex : vannes d'arrêt d'urgence) ou indirectement (ex : vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système μa l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité [14].

La probabilité de défaillance sur demande du SIS est déterminée par le calcul et la combinaison des probabilités de défaillance de ses composants. Ces probabilités dépendent des taux de défaillances des composants, des taux de défaillances dangereuses détectées et du facteur qui caractérise les défaillances de cause commune [Wikipédia].

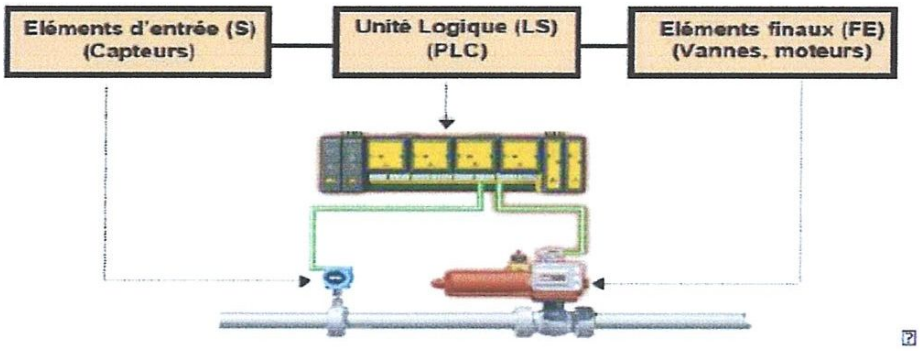

Figure 2.1 : Structure d'un système instrumenté de sécurité (SIS) [13]

Un SIS est un système visant à mettre le procédé en un état stable lorsque le procédé s'engage dans une voie comportant un risque réel (explosion, feu, . . .), [14]. Un SIS se compose de trois couches comme le montre la figure.

3. Fonction Instrumentée de Sécurité

Les principales étapes de la norme IEC 61508 [54] et ses normes filles sont déclinées dans ce qu'on appelle le cycle de vie, c'est-à-dire que ces normes traitent depuis l'analyse des risques jusqu'à l'exploitation des fonctions de sécurité instrumentées SIF (Safety Instrumented Functions).

Une SIF est définie pour obtenir un facteur de réduction du risque mise en œuvre pour un SIS. Lorsque le SIS est considère comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une fonction de sécurité [15], [10].

Un SIS contient généralement plus qu'une SIF. Si les exigences d'intégrité de la sécurité pour ces SIF diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent au SIS. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger.
L'architecture fonctionnelle d'un SIS est un ensemble de SIF qui comprend trois fonctionnalités de base, la détection, le traitement (ou la décision) et l'actionnement.

La (***figure 2.2***) illustre la définition d'un système instrumenté de sécurité et des fonctions instrumentées de sécurité qui sont exécutées. Cette figure illustre, entre autres. Une fonction instrumentée de sécurité (SIF n°1) qui protège la température de processus et fait fermer une vanne d'isolement en cas de dérive de température de procédé vers un état dangereux. Les autres fonctions instrumentées de sécurité exécutées dans cet exemple de SIS sont la protection du niveau et la protection du débit.

Une fonction instrumentée de sécurité (SIF. Safety Instrumented Function) est utilisée pour décrire les fonctions de sécurité implémentées par un système instrumenté de sécurité. Une fonction instrumentée de sécurité peut être considérée comme une barrière de protection fonctionnelle lorsque le système instrumenté de sécurité est considéré comme un système réalisant cette barrière de sécurité [29].

Une fonction instrumentée de sécurité est à réaliser par un système instrumenté de sécurité (ou par une combinaison des composantes de ce système), par un système relatif à la sécurité basé sur une autre technologie ou par un dispositif externe de réduction de risque.

Une fonction instrumentée de sécurité est spécifiée pour s'assurer que les risques sont maintenus à un niveau acceptable par rapport à un événement dangereux spécifique.

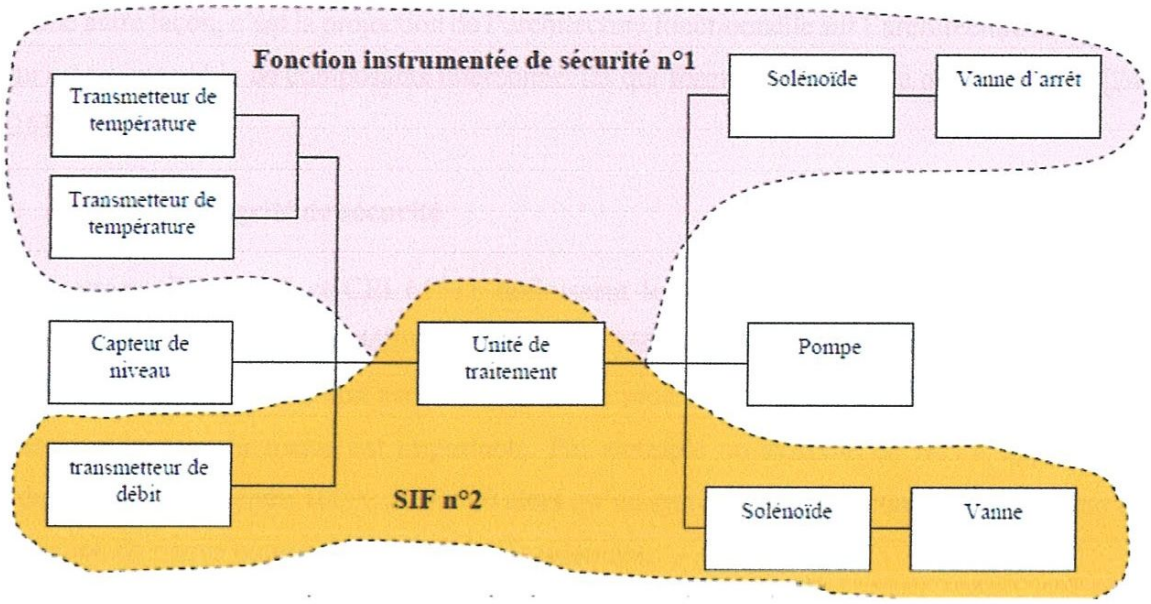

Figure 2.2 : Fonction instrumenté de sécurité

Un système instrumenté de sécurité contient habituellement plusieurs fonctions instrumentées de sécurité. Si les exigences d'intégrité de la sécurité pour ces fonctions instrumentées de sécurité diffèrent. Alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent à l'intégralité du système instrumenté de sécurité, sauf si l'implémentation garantit une indépendance suffisante entre les fonctions de sécurité. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à réduire la fréquence d'occurrence du danger. Les probabilités de défaillance des différentes fonctions de sécurité ne peuvent s'additionner que si les fonctions sont indépendantes entre elles. Dans ce mémoire. Nous prenons comme hypothèse que chaque SIS ne peut réaliser qu'une seule SIF.

L'architecture fonctionnelle d'un système instrumenté de sécurité qui est composée d'un ensemble de fonctions instrumentées de sécurité est constituée de trois fonctionnalités de base, la détection (ou la mesure), la décision et l'actionnement.

Les exigences de niveaux d'intégrité de sécurité sont allouées aux fonctions instrumentées de sécurité spécifiques. Pour évaluer l'intégrité de sécurité d'un point de vue matériel. Il est nécessaire de faire une analyse des configurations de l'architecture matérielle supportée par la fonction instrumentée de sécurité spécifiée [25].

FONCTIONNEMENT A LA SOLLICITATION		
Niveau d'intégrité de sécurité (SIL)	**Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})**	**Réduction de risque cible (RR)**
4	$10^{-5} \leq PFD_{avg} < 10^{-4}$	$100\,000 \leq RR < 10\,000$
3	$10^{-4} \leq PFD_{avg} < 10^{-3}$	$10\,000 \leq RR < 1\,000$
2	$10^{-3} \leq PFD_{avg} < 10^{-2}$	$1\,000 \leq RR < 100$
1	$10^{-2} \leq PFD_{avg} < 10^{-1}$	$100 \leq RR < 10$

Tableau 2.1 : Niveaux d'intégrité de sécurité : Probabilité de défaillances lors d'une sollicitation.

5. Normes relatives aux systèmes instrumentés de sécurité

5.1 Norme CEI 61508

En 1984, le comité technique 65 de la CEI a commencé une tâche de définition d'une nouvelle norme internationale relative à la sécurité. Cette norme CE1 61508 [CEI 00] est la seule norme multisectorielle traitant de l'ensemble de la problématique des systèmes électriques, électroniques et programmables E/E/EP, c'est-à-dire qu'elle traite à la fois le matériel et le logiciel. C'est également la seule norme très technique qui apporte des clés, auxquelles il suffit de se conformer pour atteindre un objectif. Cette norme est orientée performances en laissant à l'utilisateur le soin de réaliser son analyse de risque et elle lui propose des moyens pour réduire ce risque. Elle ne concerne pas les systèmes simples, pour lesquels le mode de défaillance de chaque élément est clairement défini et pour lesquels le comportement du système peut être totalement déterminé dans le cas d'une défaillance. Par exemple, un système comportant des fins de course et des relais électromécaniques reliés à un disjoncteur peut être étudié sans avoir recours à la CE161508.

La norme CEI 61508 repose sur deux concepts qui sont fondamentaux vis-à-vis de son application : le cycle de vie en sécurité et les niveaux d'intégrité de sécurité.

Cette norme s'applique aux systèmes relatifs à la sécurité lorsque l'un ou plus de ces systèmes comporte des dispositifs électriques/électroniques/électroniques programmables. Elle comprend 7 parties :

l. Définition des prescriptions générales qui sont applicables à tous types de matériel.

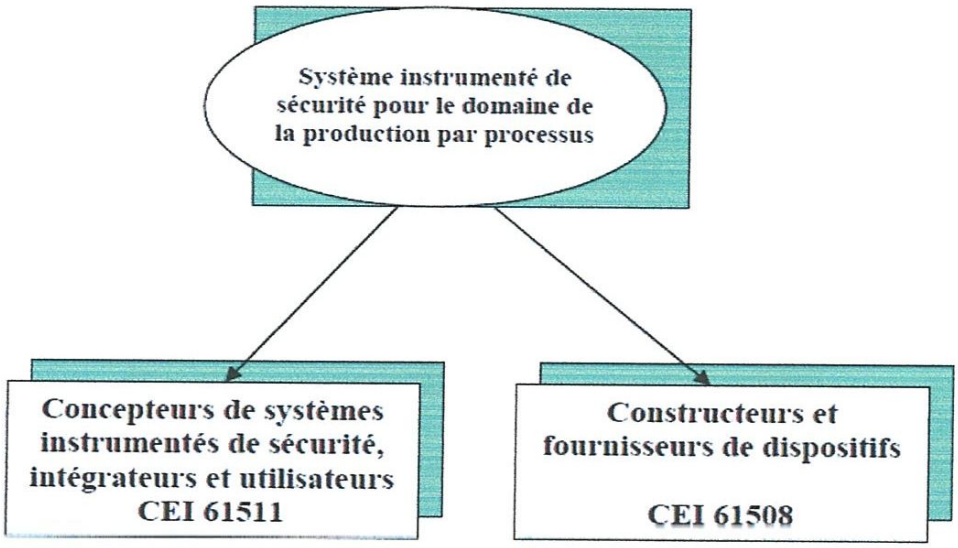

Figure 2.4 : Relation entre la CEI 61508 et la CEI 61511

La norme CEI 61511 restreint le périmètre aux systèmes pour des applications SIL 1 à 3 (les applications SIL 4 ne pouvant être traitées par un SIS seul). Les applications qui nécessitent l'utilisation d'une fonction instrumentée de sécurité de niveau d'intégrité de sécurité SIL 4 sont rares dans l'industrie de processus. Ces applications doivent être évitées en raison de la difficulté d'atteindre et de maintenir de tels niveaux élevés de performance tout au long du cycle de vie de sécurité [27].

La CEI 61511 a une volonté de simplification de la CEI 61508 en reprenant cette dernière mais en la limitant strictement aux éléments pertinents pour l'industrie des procédés continus.

désignation d'objectifs aussi, bombardement peu, attaque très occasionnellement... pas de combat aérien, peu de transport, quelques acrobaties, mais uniquement en laboratoire.

a) **Applications civiles**

Un certain nombre de travaux de recherche, certains financés par la Commission européenne, ont permis d'étudier les concepts d'applications futures possibles des drones dans le domaine civil. Les drones sont certainement une alternative technologique sérieuse à l'emploi de satellites d'observation. Plus prometteuse serait la possibilité d'employer ces engins dans des contextes d'intervention au sein d'ensembles d'agents plus complexes ou comme maillons actifs d'un réseau d'information et de décision. Un grand nombre de missions en milieu hostile pour lesquelles il faut actuellement risquer la vie de plusieurs personnes pourraient être considérées autrement si était faite la démonstration de la faisabilité de drones dotés de capacités décisionnelles suffisantes.

Les missions de surveillance sont un exemple simple : le système autonome prend en charge les tâches de pilotage et de guidage, ainsi que des tâches de veille pour lesquelles la vigilance humaine est faillible. Il soulage véritablement l'opérateur afin que celui-ci puisse se consacrer à la gestion de la mission. Au rayon des applications potentielles, on trouve pléthore de propositions, depuis la lutte anti-incendie jusqu'à la surveillance des ouvrages d'art, le tout avec, pour le moment, une foule indistincte d'appareils candidats de toutes formes et de toutes tailles. Où l'on trouve plus certainement une logique promotionnelle que pragmatique de la part des fabricants.

b) **Sécuriser l'espace aérien**

Sur ce marché émergent, des drones assez légers et de petite taille sont disponibles : quelques kilos. Ils ne sont pas très sûrs, mais ils semblent moins dangereux. Cependant, la simple rencontre d'un petit drone et d'un parebrise de véhicule pourrait engendrer un accident très grave. D'où certaines réticences justifiées. De façon générale, les besoins opérationnels ne sont pas bien exprimés, les conditions d'emploi ne sont pas précises. La réglementation actuelle reste donc très générale, très contraignante ("limitante") pour garantir la sécurité des biens et des personnes environnantes, pour le moment souvent en interdisant les drones.

c) **Une conception adaptée aux performances**

On cherche à développer l'autonomie des drones en regard des aspects liés à la conception, aux performances et à la sécurité. La conception d'un drone doit être adaptée à sa mission dans des conditions d'emploi nominales et dégradées.

En matière de performances, le drone a besoin d'une certaine intelligence embarquée pour lui permettre de percevoir, de décider et de s'adapter localement à l'environnement et aux

autres aéronefs ou agents, comme le ferait un pilote : atterrir sans danger, rattraper une rafale de vent, éviter des obstacles imprévus, éviter les autres aéronefs, etc. Enfin, au plan de la sécurité, tout système de drones doit à tout moment rester sous le contrôle des opérateurs qui le supervisent, en assurant une bonne information sur la situation. En cas d'urgence, le drone doit rester dans une enveloppe de sécurité garantie pour un retour au sol sans danger pour autrui.

Il peut être nécessaire d'avoir des drones plus autonomes pour garantir plus de sécurité, c'est probablement le facteur le plus déterminant pour le développement de l'autonomie des drones.

d) **Autonomie limitée**

La notion " d'autonomie " a ainsi été attachée au terme de " drone " de façon quelque peu abusive. On entend maintenant parler de "drones sous-marins ", " drones marins ", voire "drones terrestres ", mais c'est faire grande injustice aux robots qui peuplent nos ouvrages de science-fiction, nos usines, nos laboratoires de robotique et d'intelligence artificielle depuis fort longtemps maintenant. On peut également trouver nombre d'exemples où une tâche peut être accomplie par un drone, sans qu'il fasse preuve d'une très grande autonomie : les drones d'épandage agricole sont opérés manuellement, car la version autonome du Yamaha RMaX ne sait pas se passer d'un opérateur de sécurité au bord du champ à traiter, ni tenir compte de rafales soudaines de vent, ni faire une pause au moment du passage d'écoliers ou d'autres passants. Les drones militaires ne font guère plus que suivre leur plan de vol et les déroutements qu'on leur impose : si ce n'est poursuivre automatiquement une cible avec un capteur de désignation. La prise de décision relève du commandement et heureusement.

On distingue toutefois deux catégories de drones : ceux qui requièrent effectivement l'assistance d'un pilote au sol, par exemple pour les phases de décollage et d'atterrissage, et ceux qui sont entièrement autonomes. Cette autonomie de pilotage peut s'étendre à la prise de décision opérationnelle pour réagir face à tout événement aléatoire en cours de mission ; elle constitue la deuxième caractéristique essentielle des drones.

La vocation principale des drones est l'observation et la surveillance aériennes, vocation jusqu'à présent surtout utilisée à des fins militaires (actuellement 90% du marché mondial des drones). Ainsi, tous les drones, qu'ils soient autonomes ou non, requièrent la présence au sol d'au moins

Figure 2.10 : Drone d'incendie.

6.2.5 Des missions exploitant le vecteur aérien :

- Transport de fret.
- Largages de vivres et d'équipements de sauvetage en zones hostiles.

En 2013, la société Amazon a fait sensation en diffusant une vidéo montrant un drone livrant un colis au pied de la maison de ses destinataires. La société DIIL lui a aussitôt emboîté le pas avec une vidéo d'une livraison de colis en Allemagne. Quelques chaînes de pizzerias se sont aussi amusées à diffuser des livraisons fictives et quelques plagistes à livrer des cocktails par drone.

Livrer en un temps record, en s'affranchissant des embouteillages, telle serait la prochaine vocation des drones. Pure provocation, pour attirer l'attention des médias et des pouvoirs publics ou réalité proche ? En théorie, un drone de 8 kg peut porter 1 ou 2 kg de charge sur une vingtaine de kilomètres. Mais la technique n'est pas mûre pour être réalisée en milieu urbain : il faudrait des Lidar détecteurs d'obstacles, suffisamment petits pour être embarqués, et une centrale inertielle capable d'assurer la navigation en l'absence de signal GPS ; tout cela n'existe pour l'instant qu'en laboratoire. De surcroît, cette utilisation des drones suppose le pire des scénarios de vol pour la réglementation : vol automatique, hors vue et en zone peuplée ! À cela s'ajoute le risque de voir des drones larguer armes et drogues au-dessus des prisons, voire de commettre des actes terroristes ou même simplement de se faire détrousser de son colis !

Figure 2.11 : Drones de livraison des paquages

6.2.6 Photographie aérienne :

La photographie aérienne est l'application la plus simple. Ce type de photos constitue un solide argument pour présenter une grande propriété, un chantier ou un parc sous les meilleurs angles. C'est pourquoi les agences immobilières, les publicitaires, les professionnels du tourisme et les journalistes s'y intéressent de près. Les particuliers ne sont pas en reste.

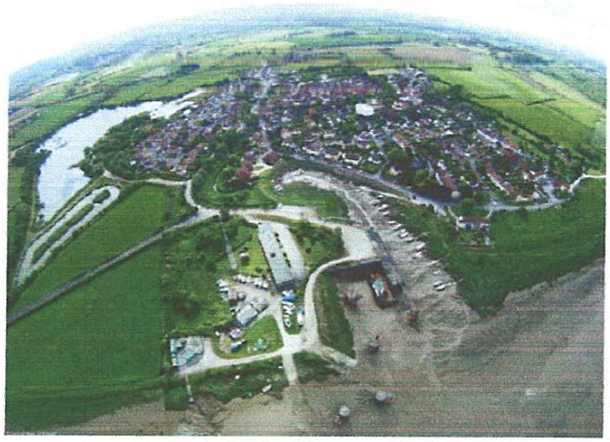

Figure 2.12 : Photographie à 150 m avec une drone

Ces applications sont évidemment susceptibles d'intéresser un large éventail de clients utilisateurs, publics et parapublics, tels que la Police, les Pompiers (évaluation de sinistres, repérage de réfugiés dans un immeuble ou sur le toit), la Sécurité civile, de nombreuses entreprises privées sont également concernées, dans les secteurs du bâtiment, des travaux publics, de la prospection (minière et pétrolière), des télécommunications, etc.

7. Les contraintes opérationnelles :

7.1 Navigabilité et intégration dans la circulation aérienne

Les drones doivent impérativement répondre à des critères de navigabilité et respecter des règles de circulation aérienne, analogues à ceux des avions. Cela leur impose de bénéficier d'un certain niveau de fiabilité technique et de résistance au crash (pour assurer la sécurité au sol) mais également d'une fiabilité satisfaisante du point de vue comportemental (pour assurer la sécurité des autres aéronefs en vol). Celle-ci doit s'exercer en matière de détection de proximité, de contrôle du pilotage, d'échange de données avec le contrôle au sol, ainsi que de la capacité de gestion des situations dégradées. C'est un problème crucial pour les drones qui, a priori, ne satisfont pas actuellement à ces contraintes.

La résolution de ces difficultés pourrait naturellement déboucher sur la création d'une certification des drones par des autorités compétentes, comme pour tous les autres aéronefs. Celle-ci apporterait certaines garanties dans les niveaux de fiabilité recherchés.

7.2 L'altitude

Si l'absence de l'homme à bord permet plus facilement l'accès aux hautes altitudes, favorables à de plus grandes portées d'observation, celles-ci posent néanmoins certaines questions relativement : aux règles de souveraineté auxquelles n'échappe que l'espace extra-atmosphérique selon le droit international, domaine exclusif des satellites ; la vulnérabilité aux menaces sol-air de hautes performances (jusqu'à 30 Km) ; une rupture technologique sur les moteurs au-delà de 20 Km.

Le drone présente un risque inhérent à ce type de système vis-à-vis de l'environnement dans lequel il évolue :

- Masse conséquente : 5 à 10 kg.
- Puissance embarquée importante (~ 2 000 W).
- Danger des hélices (6 à 8), rotation 720 t/mn.
- Pas de portance (pas de voilure), chute directe.
- Champ de vol :
  - Drones simples : max 60m.

- Drones avec autonomie avancée : entre 60m et 120m
- Zone tampon : entre 120m et 150m.
- Les grands avions : plus de 150m.

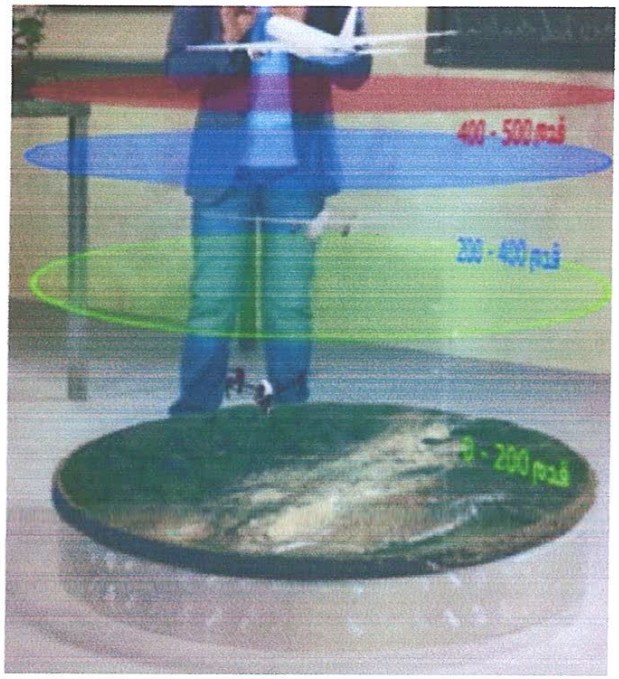

Figure 2.13 : la décomposition des champs de vol.

Le problème de l'insertion de tels engins dans la circulation aérienne civile n'est certes pas encore résolu.

Cela pose d'importants problèmes technologiques et réglementaires, tant pour l'autonomie décisionnelle embarquée ou les capteurs anticollision tout temps, que pour la gestion des vols autonomes dans les espaces aériens civils ou militaires.

8. Conclusion

Les systèmes instrumentés de sécurité sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. La norme IEC 61508 est la norme de référence pour la spécification et la conception des SIS. Sa déclinaison sectorielle dans le domaine du processus industriel [13] est destinée aux concepteurs et

utilisateurs de ce domaine. Ces normes de sécurité fonctionnelle introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés.

L'introduction de probabilité dans la mesure de niveau d'intégrité a entraîné la mise en place de nouveaux concepts tels que les notions de calculs de probabilité moyenne de défaillance à la sollicitation *PFDavg* ou de défaillance par unité de temps. Finalement, la norme reste muette sur l'aspect de la distribution de la gestion des fonctions de sécurité et sa répartition sur l'ensemble de la structure du système instrumenté de sécurité. Le vide laissé par la norme a été exploité par quelques fournisseurs qui ont profité de l'occasion pour annoncer l'utilisation de réseaux de terrain dans la fabrication des systèmes instrumentés de sécurité.

Les drones sont de plus en plus utilisés dans le domaine civil. Tous les secteurs sont concernés : le médical, Agriculture et environnement, Relevées topographiques, La surveillance et l'observation etc.

La mise en circulation des drones dans l'espace aérien peut présenter des risques sur la vie de l'être humain dans les zones urbanisées, des dangers à la circulation des avions, en cas des défauts ou des pannes qui provoque la perte de contrôle de ces drones. Pour assurer la sécurité de vol des drones et éviter les scénarios redoutés, on va étudier dans le chapitre 3 quelques méthodes d'analyse de la sûreté de fonctionnement et la sécurité.

Chapitre 3

Les Méthodes d'analyse de la sûreté de fonctionnement

1. Introduction :

Les méthodes d'analyse de la sûreté de fonctionnement (SdF) utilisent pour la plupart des systèmes une décomposition des grands systèmes en sous-systèmes ou composants individuels dont les caractéristiques sont supposées connues.

L'évaluation de la sûreté de fonctionnement d'un système consiste à analyser les défaillances des composants pour estimer leurs conséquences sur le service rendu par le système.

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 évènements susceptibles de se produire dans le système et son environnement, tels par exemple :

- Des défaillances et des pannes des composants du système.
- Des évènements 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.

On peut diviser une analyse de Sûreté de fonctionnement de système en plusieurs étapes principales, à savoir :

— L'analyse structurelle et fonctionnelle du système ;
— L'analyse qualitative du système ;
— L'analyse quantitative du système ;
— La synthèse des analyses précédentes et une conclusion.

Afin d'aider l'analyse, plusieurs méthodes d'analyse ont été mises au point. Les principales sont :

- APD : Analyse Préliminaire des Dangers,
- DdF : Méthode du Diagramme de Fiabilité s,
- MTV : Méthode de la Table de Vérité,
- AdD : Méthode de l'Arbre des Défaillances,
- MCPR : Méthode des Combinaisons de Pannes Résumées,
- MACQ : Méthode de l'Arbre des Conséquences,
- MDCC : Méthode du Diagramme Causes-Conséquences,
- MEE : Méthode de l'Espace des Etats.

Les détails et l'enchaînement de ces étapes sont donnés dans l'organigramme de la (***figure 3.1***). Il faut remarquer que ces étapes ne sont pas totalement disjointes et présentent des aspects communs.

De plus, une étude réelle est itérative, les étapes principales sont répétées plusieurs fois jusqu'à l'obtention d'une conclusion acceptable (objectifs réalisés).

La mise en œuvre de ces méthodes rend indispensables des décompositions hiérarchiques matérielles ou fonctionnelles du système.

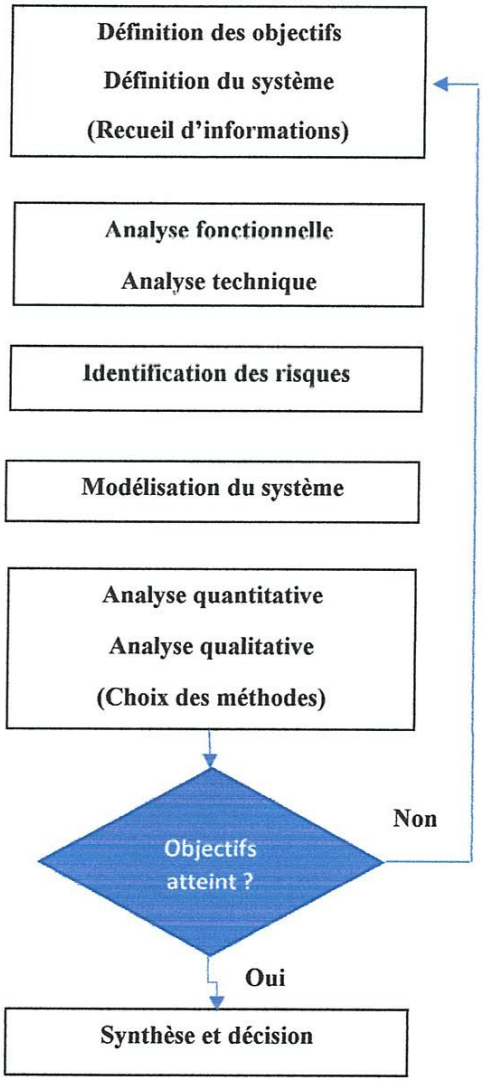

Figure 3.1: Organigramme des tâches d'une analyse prévisionnelle

2. Les méthodes d'analyses de la SdF :

2.1 L'Analyse Préliminaire des Dangers (APD)

L'analyse préliminaire des risques a été utilisée pour la première fois aux Etats-Unis au début des années soixante. Depuis, cette approche a conquis nombre de secteurs industriels tels que l'industrie aéronautique, chimique, nucléaire ou automobile.

Cette méthode a pour objectifs :

- d'identifier les dangers d'un système et de définir ses causes (entités dangereuses, situations dangereuses, accidents potentiels,).
- d'évaluer la gravité et les conséquences liées aux situations dangereuses et aux accidents potentiels.

A l'issue de cette étude, des actions correctives sont mises en œuvre afin de permettre la maîtrise ou la suppression des situations dangereuses et des accidents potentiels décelés. Il est recommandé de réaliser l'analyse préliminaire des risques dès les premières phases de conception. Cette étude sera ensuite complétée et enrichie à mesure de l'avancement dans le cycle de vie et ce, jusqu'à la fin de vie du système.

L'APG est en général une étude préliminaire nécessitant la réalisation d'études complémentaires de sûreté de fonctionnement telle que la méthode des arbres des défaillances utile à la détermination des causes des événements indésirables décelés lors de l'analyse préliminaire.

2.2 La méthode des Arbres de Défaillances (AdD)

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS [11], [20]. Elle a pour objectif le recensement des causes entraînant l'apparition de l'évènement indésirable d'un système et le calcul de sa PFD_{avg}.

Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun [22].

L'arbre de défaillances est une méthode déductive, qui commence par l'évènement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases ; une qualitative, où on détermine la fonction logique du système en termes de l'ensemble de ses

coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'évènement indésirable (sommet).

L'analyse par Arbre de Défaillance est une analyse déductive qui permet de représenter graphiquement les combinaisons d'événements élémentaires qui conduisent à la réalisation d'un événement redouté. L'Arbre de Défaillance, dont la racine correspond à l'événement redouté pour lequel on cherche à évaluer la probabilité d'occurrence, est formé de niveaux successifs tels que chaque événement soit généré à partir des événements du niveau inférieur par l'intermédiaire d'opérateurs logiques (ET, OU, ...). La décomposition s'arrête au niveau des événements élémentaires, caractérisés par le fait qu'ils sont indépendants entre eux ou que leurs probabilités peuvent être estimées ou qu'on ne désire pas les décomposer en éléments plus simples.

Un Arbre de Défaillance caractérise de façon claire les liens de dépendance, du point de vue du dysfonctionnement, entre les composants d'un système.

L'analyse par Arbre de Défaillance peut être uniquement qualitative, par recherche systématique des combinaisons minimales de défaillances entraînant l'apparition de l'événement redouté (*coupes minimales*), afin d'identifier les chemins les plus critiques, et donc d'identifier les points faibles du système. Elle peut aussi être d'ordre quantitatif ; dans ce cas, on assigne à chaque événement de base une probabilité d'occurrence pour effectuer le calcul de celle de l'événement redouté.

L'analyse par Arbre de Défaillance est largement répandue et utilisée dans les études de sûreté de fonctionnement car elle caractérise de façon claire les liens de dépendance, du point de vue du dysfonctionnement, entre les composants d'un système. En dépit de la simplicité d'utilisation de cette technique, elle souffre néanmoins de l'existence d'hypothèses implicites dont la vérification a posteriori est rarement effectuée par les praticiens. Par exemple, il est supposé que toute modification de l'ordre dans lequel les événements sont considérés n'a pas d'impact sur le scénario redouté (y compris sa probabilité d'occurrence) [5].

Evénement / report	Dénomination	Portes	Dénomination
	Evénement de base		Porte « ET »
	Evénement-sommet ou événement intermédiaire		Porte « OU »
	Report (sortie) Le sous-arbre situé sous ce « drapeau » est à dupliquer ...		Porte « OU exclusif »
	Report (entrée) ...à l'endroit indiqué par ce second drapeau		Porte « combinaison »

Tableau 3.1 : Syntaxe des arbres de défaillance.

2.3 Le Diagramme de Fiabilité (DdF)

La méthode du « diagramme de succès » ou de « fiabilité » aboutit à une modélisation fonctionnelle d'un système en considérant que les fonctions globales de ce système résultent d'une mise en série et/ou en parallèle de fonctions élémentaires. Chaque composant du système, considéré comme indépendant, réalise une fonction autonome. L'évaluation de la fiabilité du système est déduite de cette modélisation fonctionnelle.

La méthode du diagramme de fiabilité consiste à construire un diagramme composé de blocs, chacun d'eux représentant une entité (composant, sous-système, voire fonction), reliés par des arcs orientés indiquant les dépendances des entités entre elles. Le comportement des entités est binaire (fonctionnement/défaillance).

Les diagrammes sont constitués d'une entrée E, d'un « corps diagrammatique » composé « d'Entité i » et d'une sortie S. Des exemples de diagramme de fiabilité sont présentés aux figures 5 et 6. On suppose, lorsque le système fonctionne, qu'un signal est émis en E et est transmis par les arcs jusqu'à la sortie S. La défaillance d'une entité entraînera l'arrêt du signal au niveau du bloc qui lui est associé.

Un tel diagramme est une représentation statique du fonctionnement du système. L'étude consiste à chercher les combinaisons de défaillances d'entités élémentaires conduisant à la défaillance du système, appelées coupes. Les coupes ne contenant aucune autre coupe sont dites minimales.

Les règles de transmission du signal sont les suivantes :

- En série : toutes les entités doivent fonctionner pour que le signal passe (***Figure 3.2***) ;

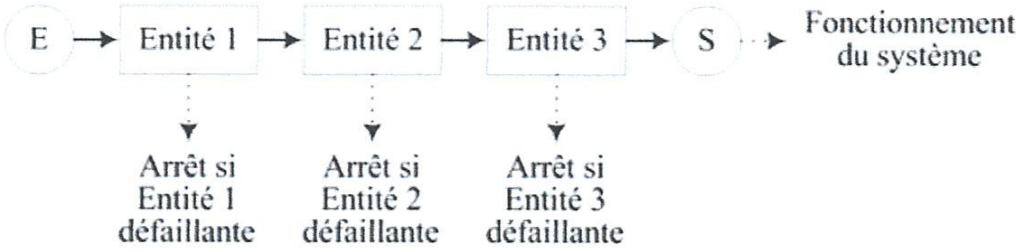

Figure 3.2 : Système en série

- En parallèle : il suffit qu'une entité fonctionne pour que le signal passe (***Figure 3.3***).

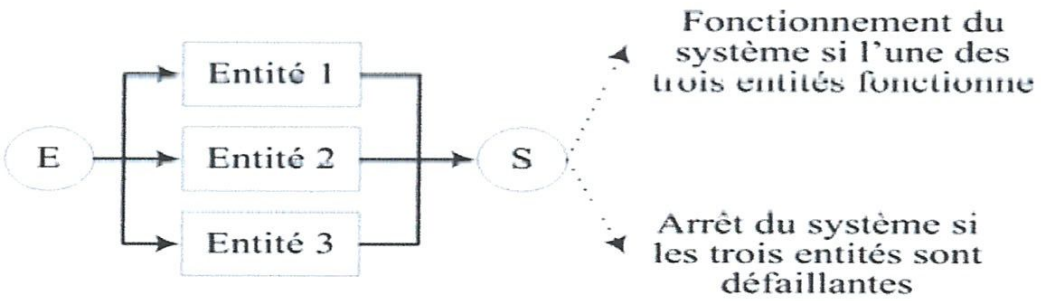

Figure 3.3 : Système en parallèle

2.4 Graphe de Markov

La méthode de graphes de Markov est utilisée pour analyser et évaluer la sûreté de fonctionnement des systèmes réparables. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et chercher comment passer d'un état à un autre lors d'un dysfonctionnement ou d'une réparation. A chaque transition, de l'état Ei vers l'état Ej, est associé un taux de transition τij défini de telle sorte que $\tau ij.dt$ est égal à la probabilité de passer de Ei vers Ej entre deux instants très proches t et t+dt sachant que l'on est en Ei à l'instant de temps t.

Les états sont classés en deux catégories :

- Des états de fonctionnement : ce sont les états où la fonction du système est réalisée, des composants du système pouvant être en panne, l'état du bon fonctionnement est l'état où aucun composant n'est en panne,

- Des états de panne : ce sont des états où la fonction du système n'est plus réalisée, un ou plusieurs composants du système étant en panne.

Le processus d'analyse comprend trois parties :

- Le recensement et le classement de tous les états du système en états de bon fonctionnement ou états de panne.
- Le recensement de toutes les transitions possibles entre ces différents états et l'identification de toutes les causes de ces transitions.
- Le calcul des probabilités de se trouver dans les différents états au cours d'une période de vie de système ou le calcul des caractéristiques de sûreté de fonctionnement.

Diagrammes de Markov

- Permet de rendre compte du comportement du système en tenant compte des évènements le rendant dynamique
- Le graphe est constitué de sommets correspondant aux différents états du système
- Les sommets sont reliés par des arcs values à l'aide de taux (ou de probabilités) de transitions non nulles associes aux évènements qui font évoluer le système

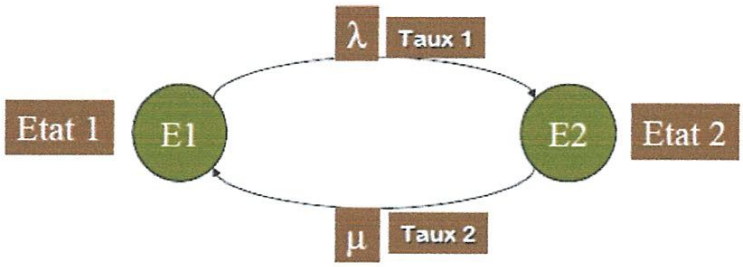

Figure 3.4 : Exemple du Graph de Markov

Un processus markovien est un processus qui modélise le comportement d'un système pour lequel l'évolution future depuis un état donné ne dépend que de cet état et non de la "trajectoire" qu'il a décrite pour y parvenir.

Intérêt des processus markoviens :

. Modélisation "fidèle" d'un grand nombre de systèmes,

. Calculs et traitements simples (si le nombre d'états n'est pas trop grand)

% Les graphes de Markov apportent une bonne formalisation de tous les états que peuvent prendre les systèmes en fonction des évènements rencontrés (défaillance, réparation,) et des paramètres étudiés (taux de défaillance, défaillance de cause commune, . . .) [23].

Les graphes de Markov apportent une finesse de modélisation pertinente au regard du comportement des SIS étudiés notamment les SIS faiblement sollicités et périodiquement testés [20]. Compte tenu de la relative complexité des SIS, l'explosion combinatoire du nombre des états est l'inconvénient majeur des chaînes de Markov. Cet inconvénient est généralement surmontable.

L'évaluation de la performance du SIS est obtenue grâce à une chaine de Markov synthétique représentant les différents états du SIS tout en tenant compte des différents types de défaillance. Elle permet de déterminer la probabilité de défaillance μa la demande du SIS et de calculer sa valeur moyenne par intégration dans le temps.

La méthode des graphes de Markov est souvent utilisée pour analyser et évaluer les performances des systèmes réparables et avec des composants a taux de défaillance constant. La construction d'un graphe de Markov consiste à identifier les différents états du système (défaillants ou non défaillants) et à chercher comment passer d'un état μa un autre lors d'un dysfonctionnement ou d'une action de réparation. Elle permet ainsi de faire une analyse dynamique du système.

Dans l'évaluation des performances des systèmes par les chaînes de Markov on utilise le processus d'analyse constitué de trois parties. La première partie est consacrée au classement de tous les états du système en états de fonctionnement, états dégradés ou états de panne. La deuxième partie concerne la détermination de toutes les transitions possibles entre ces différents états, tout en tenant compte des actions de réparations. Enfin on calcule les probabilités de se trouver dans les différents états du système étudie.

2.5 Les réseaux de Pétri :

2.5.1 Introduction :

Les réseaux de Petri constituent un outil mathématique de modélisation développé au début des années soixante par le mathématicien allemand Carl Adam Petri. Les réseaux de Petri décrivent des relations existant entre des conditions et des événements et ils modélisent le comportement de systèmes dynamiques à événements discrets [6].

Les réseaux de Petri présentent des caractéristiques intéressantes à savoir le parallélisme, la synchronisation, le partage des ressources, ...

Un réseau de Petri comporte deux types de nœuds :

- Les places qui permettent de décrire les **états** du système modélisé ;
- Les **transitions** qui représentent les **changements d'états.**

Places et transitions sont reliées par des arcs orientés. On dira qu'un réseau de pétri est un graphe biparti orienté.

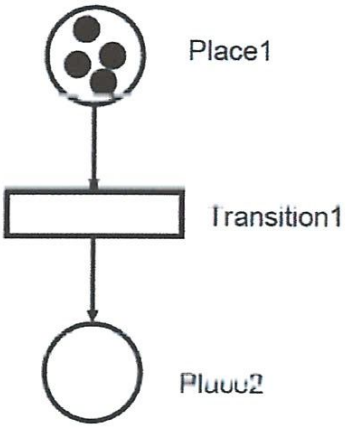

Figure 3.5 : Exemple de réseau de pétri

T1 : Transition P1, P2 : Places

2.5.2 Marquage :

Le marquage M d'un réseau de Petri est une application de P vers IN :

$$M: P \rightarrow IN$$

La (***Figure 3.5)*** représente un réseau de Petri marqué. Les places 1 et 2 contiennent des nombres entiers (positifs ou nuls) de marques ou jetons. Le nombre de marques contenu dans la place P1 est noté M(P1) et on a M(P1) = 4. Pour le même exemple, M(P2) = 0. Le marquage M du réseau entier est défini par le vecteurs de ces marquages tel que M = (M(P1),

M(P2)) = (4, 0), dans le cas de la figure précédente. L'état à un certain instant définit l'état du RdP qui reflète l'état du système modélisé par le réseau. L'évolution du marquage par franchissement des transitions dans un RdP traduit l'évolution du système modélisé dans ces différents états après l'occurrence de certains événements.

2.5.3 Franchissement et transition :

Une transition est franchissable si chacune des places en amont de cette transition contient au moins une marque [6]. Dans l'exemple précédent, la Transition 1 est franchissable ou validée.

Le franchissement (tir) d'une transition Tj consiste à retirer une marque dans chacune des places en amont de la transition Tj et à ajouter une marque dans la place en aval de la transition Tj.

Après franchissement, le RdP possède un nouveau marquage M'. Une suite de franchissements de transitions à partir d'un marquage donné est appelée séquence de franchissement.

2.5.4 Réseaux de Petri stochastiques

Les réseaux de Petri stochastiques ont été introduits afin de répondre à certains problèmes d'évaluation quantitative des systèmes informatiques industriels.

Dans les réseaux de Petri stochastiques, les délais associés aux transitions sont aléatoires contrairement aux durées déterministes et constantes associées aux RdP temporisés. Ces temps sont modélisés par des variables aléatoires dont la loi la plus courante est la loi exponentielle qui permet d'approcher le graphe des marquages à un processus markovien homogène.

Les réseaux de Petri stochastiques sont très utilisés en sûreté de fonctionnement. Le franchissement d'une transition de nature stochastique reflète l'occurrence d'une défaillance modélisée par une loi exponentielle et le passage d'un état de fonctionnement normal à un état de panne.

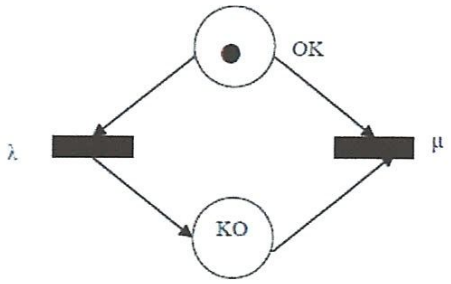

Figure 3.6 : Modélisation des états normal et de panne d'un composant

Dans ***(Figure 3.6)*** la variable λ représente le taux de défaillance du composant et la variable μ représente le taux de réparation de ce même composant.

Dans un réseau de Petri stochastique, chaque transition Ti est lui est associée une durée de franchissement aléatoire di. Cette durée correspond au temps qui s'écoule entre la sensibilisation et le tir effectif de la transition. On peut associer une fonction de répartition à la variable aléatoire (durée de franchissement) :

$$F_i(t) = 1 - e^{-\lambda_i(M)t}$$

Où le paramètre λ i(M) dépend du marquage M courant. Ce paramètre est appelé taux de transition relativement au marquage M.

2.5.5 Réseaux de Petri stochastiques généralisés

Les transitions dans les réseaux de Petri stochastiques sont associées toutes à une temporisation selon une distribution de loi exponentielle par exemple. [7] a introduit les réseaux de Petri stochastiques généralisés afin de s'affranchir de certaines restrictions.

Dans les RdPSG (réseaux de Petri stochastiques généralisés), les transitions autorisées sont de deux types et elles peuvent soient :

- Des transitions temporisées basées sur des distributions exponentielles,
- Des transitions déterministes à temporisation nulle (transition immédiate) basée sur une distribution de Dirac. Ces transitions sont franchies immédiatement dès qu'elles sont sensibilisées.

Les transitions immédiates expriment des synchronisations ou encore elles approximent des durées très faibles par rapport aux durées des transitions stochastiques.

2.5.6 Exemple :

Le principal avantage des RdP est la possibilité d'analyser le comportement d'un système en présence de défaillances. Cette modélisation dynamique permet d'obtenir des mesures en termes de fiabilité, en assignant des valeurs numériques aux paramètres du modèle. Un RdP permet de modéliser d'une part le fonctionnement normal d'un système et d'autre part les occurrences de défaillances.

On prend comme exemple Le système de l'ouverture automatique d'une portière : le conducteur du véhicule en possession de la clé est détecté par le capteur du système ce qui déclenche l'activation d'un convertisseur qui alimente le reste du système. L'information est reçue puis traitée par un processeur muni d'un RAM qui déclenche un moteur qui ouvrira la portière.

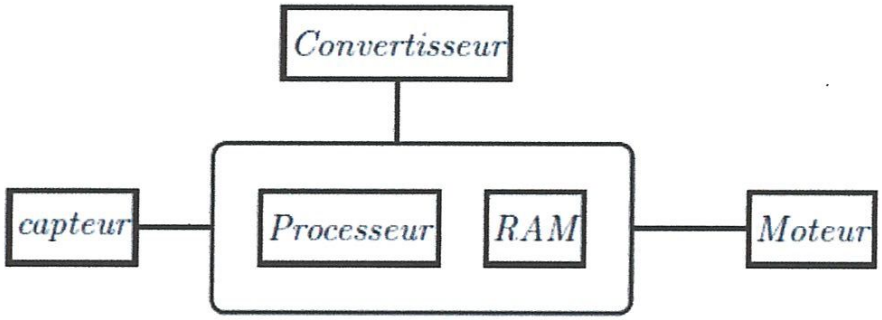

Figure 3.7 : Schéma représente le système de l'ouverture automatique d'une portière

On a modélisé le système en un réseau de Petri : chaque composant a deux états correct (état de bon fonctionnement) ou défaillance, tout équipement arrêté ne peut tomber en panne. Le système sous forme de réseau de Petri est modélisé dans la (***Figure 3.8)***.

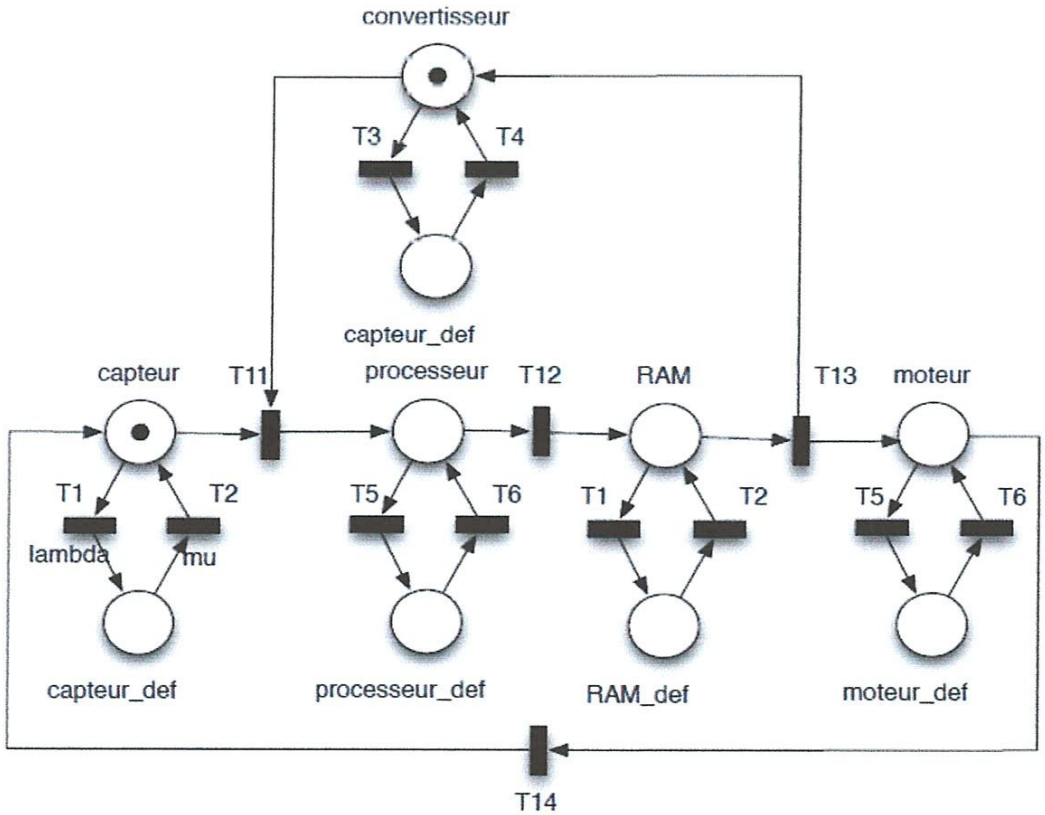

Figure 3.8 : Réseau de Petri du système

3. Détermination des niveaux de sécurité des SIS

L'évaluation du niveau d'intégrité de sécurité d'un SIS est déterminée par des méthodes qualitatives et quantitatives [18]. Elles permettent ; d'examiner les différents dangers

provenant du système opérationnel et de déterminer le SIL de la SIF pour réduire la criticité du danger analysé. L'objectif global de ces méthodes est de décrire une procédure d'identification des SIF, d'établir les niveaux de sécurité correspondant et de les mettre en œuvre dans un SIS afin de ramener le procédé dans l'état de sécurité attendue, elles ont néanmoins toutes en commun d'assurer la cohérence du classement des risques. [19].

3.1 Les méthodes qualitatives

La norme IEC 61508 introduit des méthodes qualitatives qui permettent d'allouer le SIL à partir de la connaissance des risques associés au procédé. Les méthodes les plus utilisées sont la méthode du graphe de risque [9] [18], [21] et la méthode de la matrice de gravité des évènements dangereux [20].

3.1.1 Graphe de risque :

Il s'agit de la méthode qualitative la plus répandue, elle permet de déterminer le niveau d'intégrité de sécurité d'une SIF à partir de l'analyse des risques associés au procédé [8], [15].

En général, dans le secteur des processus continus, le risque est une fonction des quatre paramètres suivants [30] :

Paramètre		Description
Conséquence	C	Nombre d'accidents mortels et/ou de blessures graves pouvant résulter de l'occurrence de l'événement dangereux. Déterminé en calculant les nombres d'accidents dans la zone exposée lorsque celle-ci est occupée en tenant compte de la vulnérabilité à l'événement dangereux.
Occupation	F	Probabilité que la zone exposée soit occupée. Déterminée en calculant la fraction de temps d'occupation de la zone. Il convient de prendre en compte la possibilité d'une probabilité accrue de personnes se trouvant dans la zone exposée afin de rechercher les situations anormales pouvant exister lors de la progression vers l'événement dangereux.

Probabilité d'éviter le phénomène dangereux	P	Probabilité que des personnes exposées peuvent éviter la situation de phénomène dangereux qui existe si la fonction instrumentée de sécurité échoue à la sollicitation. Dépend s'il existe des méthodes indépendantes d'alerte des personnes exposées au phénomène dangereux et s'il existe des moyens pour y échapper.
Taux de demande	W	Nombre de fois par an que l'événement dangereux se produit si aucun système instrumenté de sécurité n'a été adapté. Peut être déterminé en considérant toutes les défaillances pouvant générer l'événement dangereux et en estimant le taux global d'occurrence.

Tableau 3.2 : Paramètres de risques relatifs au danger

L'affectation de valeurs numériques aux paramètres du ***(Tableau 3.2)*** constitue la base de l'évaluation du risque de procédé qui existe en l'absence de la fonction instrumentée de sécurité concernée.

Le graphe ou diagramme de risque (***Figure 3.9)*** associe des combinaisons particulières des paramètres de risque aux niveaux d'intégrité de sécurité. La relation entre les combinaisons des paramètres de risque et les niveaux d'intégrité de sécurité est établie en prenant en compte le risque tolérable associé à des phénomènes dangereux spécifiques.

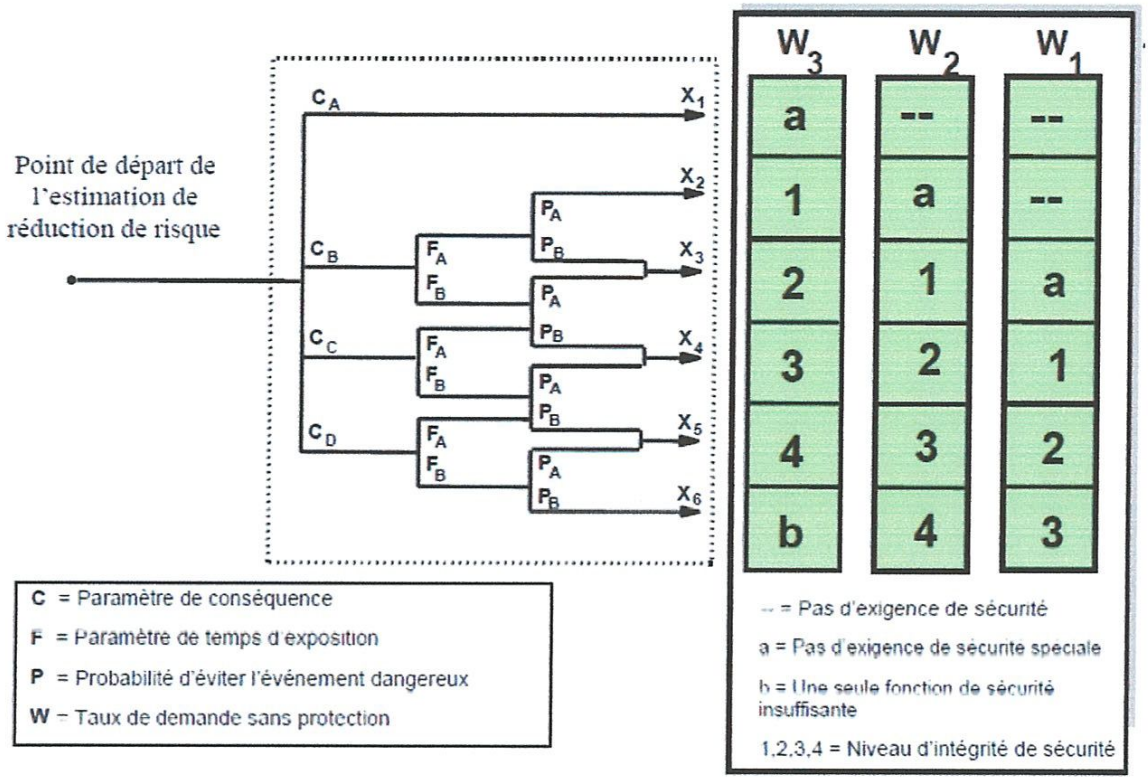

Figure 3.9 : Schéma général de graphe de risque

3.1.2 Matrice de risque

Contrairement à la méthode du graphe de risque qui ne prend en compte qu'une fonction de sécurité, la matrice de risque intègre plusieurs fonctions de sécurité sous réserve de leur indépendance [12]. La matrice possède trois dimensions : la gravité, la probabilité d'occurrence de l'accident potentiel et le nombre de dispositifs de sécurité qui sont déjà mis en place pour empêcher le développement du danger en un accident [8]. Comme déjà mentionné pour la méthode de graphe de risques, la structure de la matrice de risque dépend du domaine spécifique d'activité [9].

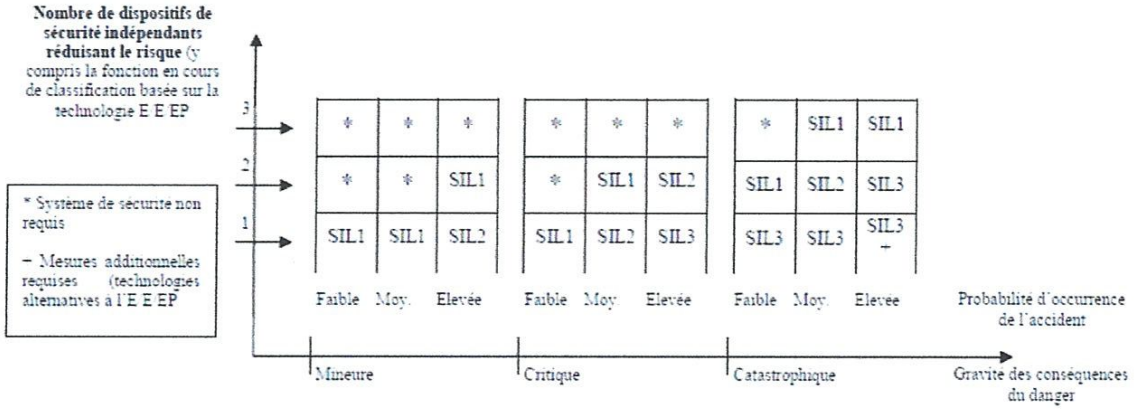

Figure 3.10 : Exemple de matrice de risque

L'exemple représenté sur la (***Figure 3.10)*** est tiré de la norme CEI 61508. Suivant la mise à disposition d'1m dispositif de sécurité permettant la prévention d'un danger d'occurrence faible et dont les conséquences sont critiques, le niveau d'intégrité de la fonction de sécurité sera réalisé en tenant compte des exigences relatives au SIL 1.

3.2 Les méthodes quantitatives

Les normes de sécurité fonctionnelle, l'IEC 61508 [12] et l'IEC 61511 [13], introduisent une approche probabiliste pour l'évaluation quantitative de la performance du SIS et la qualification de cette performance par des niveaux de sécurité référencés [19]. L'introduction de probabilité dans la mesure du niveau d'intégrité a entraîné la mise en place de concepts tels que les notions de calcul de probabilité de défaillance à la sollicitation ou de défaillance par unité de temps [20].

3.2.1 Les équations simplifiées

Les normes de sécurité fonctionnelle n'imposent cependant pas l'utilisation de modèles particuliers mais fournissent des formules approchées pour les architectures courantes. En effet, la communauté des fiabilistes s'est rendu compte que certaines équations citées dans la norme IEC 61508-6 [12] ne sont valables que sous plusieurs hypothèses qui ne sont pas citées dans la norme [19]. En outre, ces formules ne sont valables que pour certains types d'architecture k parmi n. D'après Innal [14], les équations simplifiées sont utilisées pour l'étude d'architectures de SIS dont les canaux sont mutuellement indépendants et homogènes [14], [19].

Comme mentionné par plusieurs chercheurs dans le domaine de la fiabilité des systèmes

[18], [14], il est nécessaire d'utiliser des méthodes de sûreté de fonctionnement classiques telles que les diagrammes de fiabilité [16], les arbres de défaillances [18], ou les approches markoviennes [14] pour évaluer les performances des SIS (la PFD_{avg} et le SIL), plutôt que d'utiliser les équations simplifiées données dans la partie six de la norme IEC 61508 [12].

3.2.2 Blocs diagramme de fiabilité

La méthode de diagramme de fiabilité est une représentation de la logique de fonctionnement des systèmes. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste μa rechercher les liens existants entre ces blocs [16]. Elle permet une analyse quantitative qui a pour objectif en particulier de définir la probabilité de bon fonctionnement d'un système. Les calculs reposent sur les probabilités de réussite des missions des éléments constituants le système. Cette méthode est utilisée dans l'évaluation des performances des SIS par le calcul de la PFD_{avg} résultante et la détermination du son niveau SIL [11].

La méthode de bloc diagramme de fiabilité a ses limites d'application : il faut s'assurer de l'indépendance entre les différents états de fonctionnement, elle ne permet pas de modéliser des systèmes dynamiques, sauf sous certaines conditions.

4. Comparaison des méthodes d'analyse

Pour identifier la meilleure méthode pour fiabiliser un système mécatronique, nous comparons les principales caractéristiques des méthodes. Nous excluons de cette comparaison l'APR considérée plutôt comme une méthode préliminaire et la TV qui devient vite inutilisable par l'explosion de combinaisons possibles pour plusieurs états de fonctionnement et de panne des composants.

La comparaison a été faite sur un ensemble de critères caractérisant la fiabilité d'un système mécatronique. Nous avons retenu les critères suivants :

- Moyens de représentation associés à la méthode (moyens spécifiques de représentation du système mécatronique) ;
- Système mécatronique irréparable (pour un tel système, tous les composants sont considérés comme irréparables) ;
- Système mécatronique réparable (pour un tel système, tous les composants sont considères comme réparables) ;
- Système statique ;

- Système dynamique ;
- Comportement dysfonctionnel d'un système mécatronique ;
- Comportement fonctionnel d'un système mécatronique ;
- Modélisation par niveau du système.

Dans le (***Tableau 3.3***), nous désignons par un '+' le fait que la méthode possède la caractéristique et par un '-' le contraire.

Méthodes / Caractéristique	AdP	DF	RdP
Système irréparable	+	+	+
Système réparable	+	+	+
Système dynamique	-	-	+
Comportement fonctionnel du système	-	-	+
Comportement dysfonctionnel du système	+	+	+

Tableau 3.3 : Comparaison des méthodes.

La comparaison montre à nouveau que la méthode RdP présente beaucoup d'avantages, elle est la seule qui est utilisable aussi bien pour des systèmes mécatroniques irréparables que réparables. Elle prend en compte, d'une part, des stratégies complexes de réparation, et, d'autre part, permet de considérer à la fois le comportement dysfonctionnel et fonctionnel des systèmes mécatroniques. La modélisation du système par niveau est relativement simple. De plus, les RdP sont la seule méthode qui permet d'englober l'aspect dynamique, qui est essentiel dans les systèmes mécatroniques.

5. Conclusion :

Dans ce chapitre, nous avons présenté quelques méthodes d'analyses de la sûreté de fonctionnement pour la détermination de niveau d'intégrité de sécurité, une comparaison entre ces méthodes a été réaliser dans ce chapitre, est on a conclu que l'étude de la sûreté de fonctionnement par le modèle RdPS a beaucoup d'avantage et permet de considérer à la fois le comportement dysfonctionnel (aspect stochastique) et fonctionnel des systèmes étudier.

Chapitre 4

Cas d'application : Drone de surveillance

HERCULES 5 UF

1. Introduction :

Dans ce chapitre, deux méthodes d'évaluation de la sûreté de fonctionnement d'un système SIS sont proposées. Le premier est l'AMDE, cette méthode informelle repose sur l'établissement d'un tableau décrivant les modes de défaillances des éléments du système étudié et leurs effets, éventuellement complétés par les mécanismes de détection et de reconfiguration. Il existe plusieurs types d'AMDE dont l'AMDE fonctionnelle qui permet d'identifier les conséquences d'une simple faute. Les étapes de sa construction intègrent : l'association d'un mode de défaillance à chaque fonction du système, l'identification de scénarios de panne (ou conditions de panne) et la détermination des conséquences des modes de défaillance. Des probabilités d'occurrence de panne peuvent être affectées aux éléments fonctionnels à partir du modèle RdPS couplé par des lois de fiabilité déterminer à partir de l'AMDE. L'objectif est d'évaluer les paramètres de la sûreté de fonctionnement d'un drone de surveillance HERCULES 5 UF c'est l'objectif de la section suivante.

2. Généralité :

Les systèmes de drones actuels sont dotés de peu de capacités décisionnelles embarquées. Leur mise en œuvre impose des contraintes de maintien des liaisons, de permanence du contrôle et de vigilance des opérateurs qui limitent grandement les missions pouvant être réalisées.

Ils sont de ce fait limités en portée, détectables, vulnérables à la perte de liaisons, peu discrets, peu réactifs, peu manœuvrant et cantonnés à des missions militaires de reconnaissance, d'observation pour le renseignement ou de désignation d'objectifs (à comparer avec l'utilisation des aéronefs en 1914). Les drones ne sont pas utilisés dans le domaine civil du fait de problèmes de sécurité, de certification des aéronefs, de réglementation aérienne et d'insertion dans la circulation aérienne civile (« voir et éviter »).

Les petites et moyennes entreprises innovantes développant des drones n'ont pas les moyens de développer une avionique utilisant des techniques avancées d'acquisition, de traitement de l'information et de décision autonome.

Le risque technologique inhérent aux efforts de recherche encore nécessaires est trop grand pour les industriels du domaine aérospatial. De ce fait, les industriels aéronautiques développent des drones qui ne sont pas plus autonomes, même s'ils emportent des composants plus riches.

De fait, les utilisateurs potentiels de drones autonomes ne peuvent pas se faire une idée claire des potentialités de tels systèmes, faute de l'existence de démonstrateurs finalisés et volants.

Le marché peine à se définir et les donneurs d'ordre étatiques n'ont pas une visibilité suffisante sur l'état des techniques pour engager des projets sur des technologies très en amont du savoir-faire actuel et sur des besoins imparfaitement définis pour le moment.

3. Drone de surveillance HERCULES 5 UF :

Si l'Armée assure depuis plusieurs années des missions de renseignement et d'intervention grâce aux drones, la sécurité civile commence seulement à utiliser les drones.

Délaissant la simple photographie aérienne, qui représente encore 80% de l'offre, les fabricants de drones sont de plus en plus nombreux à se tourner vers le marché de la sécurité autour d'applications de plus en plus pointues comme :

- L'inspection d'ouvrages et infrastructures pour la prévention des accidents et l'entretien : la thermographie aérienne par exemple vise à repérer les points d'infiltration d'eau, les ruptures de canalisation ou encore les erreurs de construction depuis l'extérieur d'un bâtiment. Un drone peut aussi examiner de près les installations difficiles d'accès (barrage, pylône, pipeline).

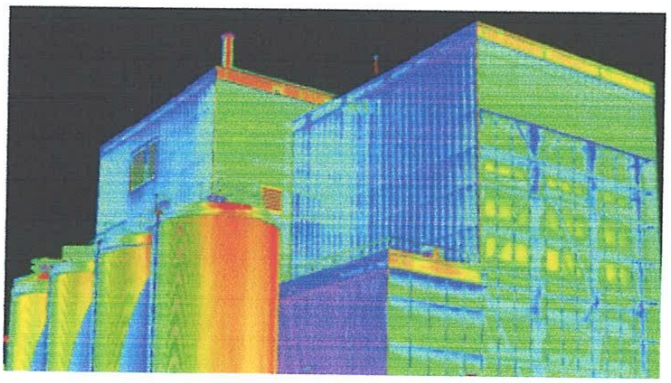

Figure 4.1 : vue thermographique.

- La détection radionucléaire.
- La gestion de crise : les drones permettent d'obtenir une vision globale de la situation afin de pouvoir coordonner les différents intervenants.
- L'aide en cas d'urgence, d'intempéries, de catastrophe naturelle ou de plan Orsec afin d'établir un constat photographique des dégâts matériels, voire un bilan humain précis.
- En Sécurité urbaine, le drone peut permettre le suivi d'une manifestation, en plein air et en milieu urbain.

- La surveillance des feux de forêt au plus près en complément aux moyens aériens existants.

Figure 4.2 : Drone de surveillance HERCULES 5 UF

3.1 Principaux composants :

Ouvrons maintenant le châssis d'un drone pour en découvrir les composants. Parmi les systèmes de bord. L'autopilote et ses capteurs occupent une place centrale, suivis de la motorisation, des actionneurs et de la transmission.

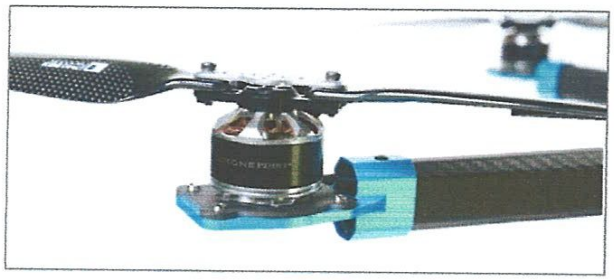

Figure 4.11: Moteur synchrone sans balais

Les moteurs brushless ont un rendement proche de 90 % et ne demandent pas d'entretien. Ils peuvent même fonctionner sous l'eau. Il en existe deux sortes : les moteurs à cage tournante, les plus répandus car offrant un bon couple, et les moteurs à cage fixe qui peuvent être noyés dans un fuselage.

Quatre moteurs brushless sont nécessaires pour le quadrirotor. Ils en existent de différentes taille et puissance. Ils sont caractérisés par le diamètre de leur cage tournante et par le nombre de tours/volt ou KV. Un moteur ayant un KV de 1000 tr/V fonctionnera à 12000 tours/min s'il est alimenté en 12V. Sur les moteurs brushless utilisés en modélisme, les bobinages en cuivre sont montés sur le stator et les aimants sur le rotor, à l'inverse des moteurs électriques conventionnels.

3.5.2 Hélices

Les hélices des drones sont les pneus des voitures, des pièces d'usure à surveiller. Les multi rotors fonctionnent avec des paires d'hélices à pas normal (horaire) et à pas inversé (antihoraire).

Il faut respecter le type de pas, sous peine de voir le multi rotor se retourner au décollage.

Les matériaux utilisés sont par ordre croissant de prix et de performance : le nylon (plastique), le bois (généralement le hêtre), et le carbone. Les hélices en bois ont le mérite d'être moins dangereuses en cas de choc. Le métal, réservé à l'aviation générale, est utilisé pour les drones de grande taille. L'hélice peut être fixe ou repliable pour prévenir la casse. Il est pratique de pouvoir replier ces éléments fragiles lors du transport, ce qui offre un gain de place appréciable.

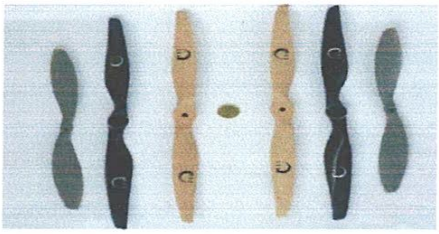

Figure 4.12 : Hélices en carbone [noires]. Hêtre [beiges] ou nylon [grises]

Les hélices peuvent grièvement blesser, même à bas régime. Il faut toujours les retirer pour un essai de rotation des moteurs après un changement de logiciel ou d'électronique et se dire que, dès que la batterie est branchée, il y a un risque qu'un moteur démarre inopinément.

3.6 La caméra

Elle permet soit de d'enregistrer le vol pour le visionner plus tard.

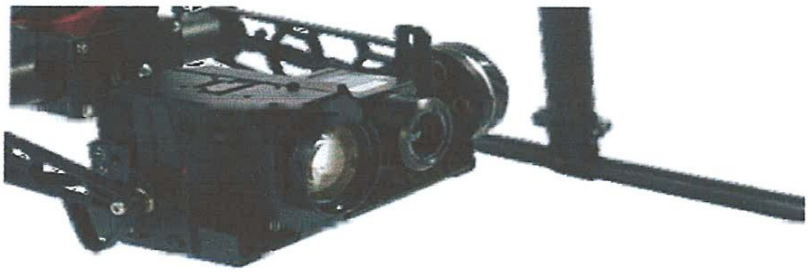

Figure 4.13 : Caméra GoPro.

Cette caméra entièrement stabilisée est dotée d'un zoom optique x18 qui permet d'analyser la scène plus en détail ou d'examiner à distance sans exposer le drone au danger. La caméra avec zoom x18, entièrement contrôlable en pitch, ouvre un vaste éventail de possibilités pour une vision précise en gardant une distance de sécurité. Idéal pour les travaux d'inspection pour lesquels les vues rapprochées sont une nécessité.

3.7 Caméra thermique

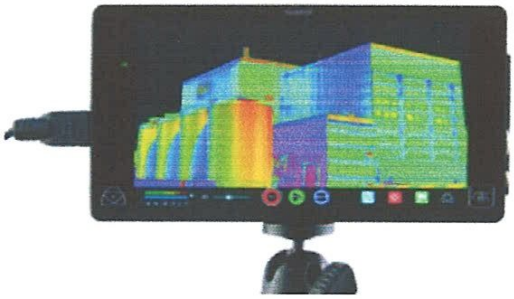

Figure 4.14 : FLIR vue pro Thermique.

FLIR vue pro 640×480 9hz, une imagerie optimisée pour les opérations aériennes réalisables dans de nombreux types d'environnements.

Le FLIR VUE PRO enregistre des vidéos numériques 8 bits en format MJPEG ou H.264 et des images fixes 14 bits sur une carte micro-SD amovible afin de ne perdre aucune de vos données en cas de perte de transmission.

4. Principe de fonctionnement du drone HERCULES 5 UF :

Le schéma de commande du drone (cas d'application) est représenté par la figure suivante :

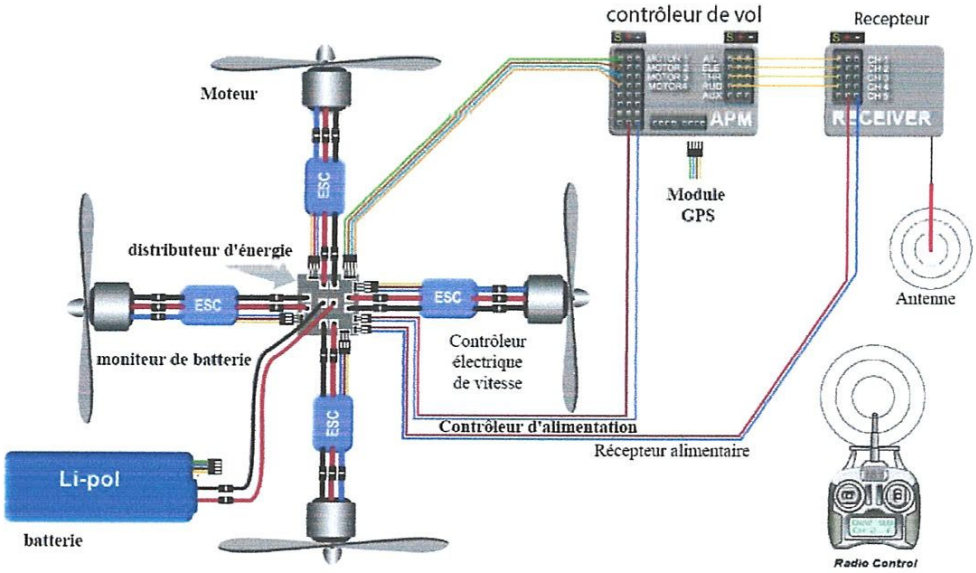

Figure 4.15 : Schéma de commande du drone.

Le schéma de principe de fonctionnement simplifié du cas d'application est donné par la ***Figure 4.16***.

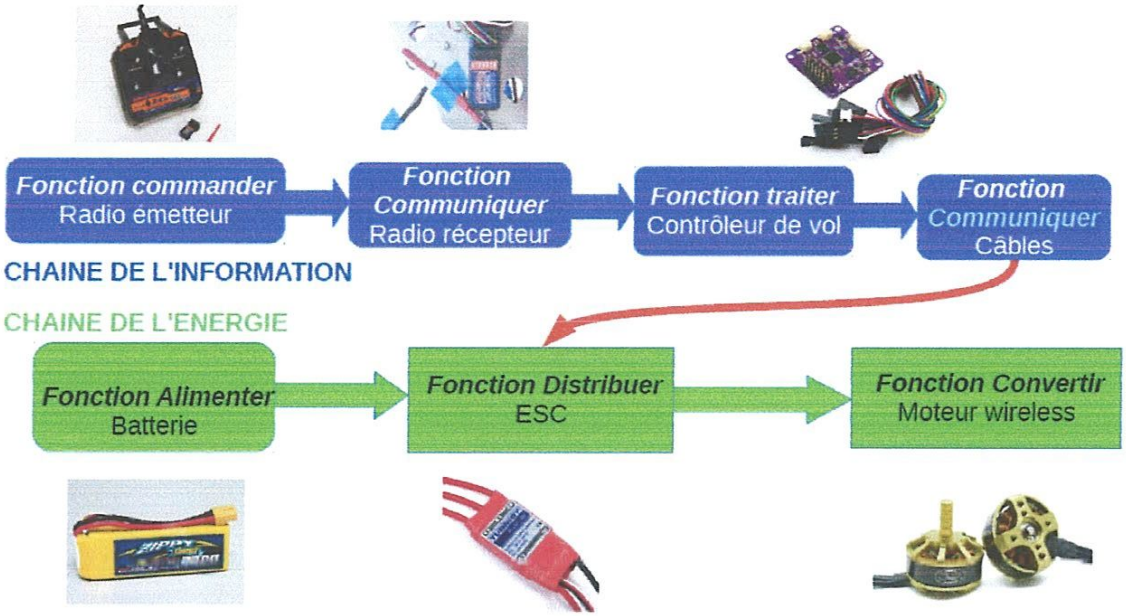

Figure 4.16 : Schéma fonctionnel simplifié

5. Etude de la Sûreté de Fonctionnement du cas d'application

L'étude de la SdF d'un système n'est possible que si son comportement fonctionnel et dysfonctionnel peut être décrit par un formalisme adopté.
Les réseaux de Petri stochastiques conduisent à des modèles qui peuvent être facilement simulé. Pour chaque composant, les temps de défaillance obtenue par simulation permettent de déterminer les paramètres des lois de fiabilité associées.
La connaissance de la fiabilité prévisionnelle de chaque composant permet d'identifier au plus tôt le composant « fragile » et d'apporter des modifications à la conception du système. Afin de facilité la construction du modèle RdPS on commence de cite les modes de défaillance et les symptômes ainsi que l'AMDE du cas d'application.
La méthode de recherche des scénarios redoutés proposée est obtenue par une nouvelle méthode utilisant le couplage entre le model RdPS couplé avec des lois de fiabilité utilisons le logiciel GreatSPN Editor. Dans la section suivante on étudier les différents modes de défaillance ainsi que l'AMDE du cas d'application.

5.1 Modes de défaillance :

L'étude de la sûreté de fonctionnement du Drone est basée sur ces modes de défaillances elle conduit à pouvoir évaluer le comportement global du système.
A cet instant, le défi est de rassembler les connaissances sur les façons dont le système pourrait devenir défaillant. La seule donnée d'entrée disponible est la connaissance purement fonctionnelle du système avec des descriptions structurelles et comportementales.
On cherche alors à rassembler les modes de défaillances des unités fonctionnelles ou des composants du système afin d'enrichir la connaissance du système mis en place.
Une liste des défaillances possibles du cas d'application drone (***Tableau 4.1***), classées par rapport au composant et aux modes de défaillances est rassemblé dans le ***Tableau 4.1***.

Périmètre	Symptômes	Hypothèses	Actions
Démarrage	Aucun moteur ne démarre.	La commande n'est pas sur le bon canal	Vérifier que la commande est bien sélectionnée.
		Les moteurs n'arment pas.	Calibrer la radio : s'assurer que les valeurs atteignent le minimum et le maximum prescrits.
		Batterie à plat	Vérifier l'état des batteries.
	Un ou plusieurs moteurs ne tournent pas.	Le drone n'étant pas à plat, le moteur situé en amont ne démarre pas.	Mettre le drone à plat.
		La chaîne autopilote-ESC (contrôleur électrique de vitesse) -Moteur est défectueuse.	Vérifier l'arrivée de courant avec un voltmètre, ou réaliser un test avec un autre moteur, ou ESC. Remplacer l'élément défectueux
		Le type de drone sélectionné dans l'autopilote ne correspond pas à celui employé.	Vérifier
		Moteur obstrué	Des herbes peuvent s'être enroulées, nettoyer
Vol	Le drone se retourne au décollage.	Une hélice horaire mise à la place d'une hélice antihoraire et vice versa.	Remplacer l'hélice.
		Un moteur tourne dans le mauvais sens.	Invertir 2 câbles sur 3 entre l'ESC et le moteur, ou inverser le sens depuis le logiciel
			Vérifier si le moteur est relié à la bonne sortie de l'autopilote.
			Vérifier si le type de drone a été correctement sélectionné dans le logiciel de vol.
		L'autopilote est mal installé.	Vérifier qu'il est installé dans le bon sens, sans jeu et protégé des vibrations.
	Le drone est instable	Le PID est instable	Vérifier.
		Les commandes sont trop sensibles : le pilot sur réagit.	Régler la courbe de course des servos depuis le télécommande : mettre des exponentiels pour adoucir les actions près du neutre.
		Le châssis n'est pas rigide.	Vérifier l'intégrité de la structure, serrer les vis.
		La batterie s'est épuisée	Vérifier l'état de la batterie
		Le drone est en surcharge	Vérifier le poids

	Le drone part dans la mauvaise direction commande inversées	Commande inversées	Inverser la course des servos depuis la télécommande
	Le drone part dans une direction et ne peut être ramené	Drone déséquilibré	Vérifier l'équilibre. Le cas échéant, déplacer des composants du drone.
	Le position Hold ne tient pas	Peu ou pas de réception GPS	Vérifier le nombre de satellites et la puissance du signal GPS
		Le drone effectue des cercles concentriques.	Calibrer le compas. Vérifier le PID.
	L'altitude Hold ne tient pas	Surcharge	Vérifier le poids et/ou modifier la courbe des gaz
		La batterie s'épuise	Vérifier
		L'accéléromètre est perturbé	Calibrer l'accéléromètre
		Le compas est perturbé	Calibrer le compas
Charge utile	Pas de retour vidéo	L'émetteur vidéo et le récepteur ne sont pas sur le même canal	Modifier la fréquence de réception en utilisant les interrupteurs
		Batterie de la caméra à plat	Vérifier
		La chaîne : prise HDMI-convertisseur numérique vers analogique-émetteur vidéo, est défectueuse ou mal alimentée	Vérifier la connexion et l'alimentation
	Image instable	Vibration du ou des moteurs	Vérifier l'état des isolateurs de la nacelle et équilibrer le hélices
	La caméra n'arrive pas à garder une position stable de haut en bas	La caméra n'est pas fixée sur son centre de gravité	Vérifier que la caméra est fixée sur son centre de gravité

Tableau 4.1 : Les modes de défaillance et les symptômes.

5.2 Principe de la méthode d'analyse de la SdF

C'est au cours des premiers vols que les problèmes de montage ou de paramètres arrivent à mettre le système à l'état de défaillance. Il s'agit le plus souvent de problème de connexion ou d'alimentation. Plusieurs causes peuvent avoir les mêmes symptômes. Il faut émettre des hypothèses et les vérifier une à une. Réaliser des tests avec des composants de remplacement

neufs permet aussi de gagner du temps. Pour l'exercice, imaginons que les vols ont lieu par un jour sans vent et que les batteries ont été rechargées.

5.3 Méthode d'évaluation de la sécurité (AMDE) :

On distingue plusieurs méthodes d'évaluation de la SdF et de la sécurité. L'analyse des modes de défaillances, de leurs effets (AMDE) est une méthode de type inductif qui s'utilise aisément lors d'une analyse préliminaire de risques. Cette méthode informelle repose sur l'établissement d'un tableau décrivant les modes de défaillances des éléments du système étudié, leurs effets et leur criticité, éventuellement complétés par les mécanismes de détection et de reconfiguration. Il existe plusieurs types d'AMDE dont l'AMDE fonctionnelle qui permet d'identifier les conséquences d'une simple faute. Les étapes de sa construction intègrent : l'association d'un mode de défaillance à chaque fonction du système, l'identification de scénarios de panne (ou conditions de panne) dans un contexte efficace et la détermination des conséquences des modes de défaillance. Des probabilités d'occurrence de panne peuvent être affectées aux éléments fonctionnels pour des traitements résultants par le modèle RdPS couplé par des lois de fiabilité par exemple.

Le ***(Tableau 4.2)*** présente l'AMDE pour le système de contrôle de drone.

Phase	**Vol à vue en zone non habitué**
Mode de panne	Perte du contrôle manuel en zone non habitué
Cause possible	(1) calculateur défaillant, (2) liaison bord-sol défaillant, (3) changement de mode involontaire par le pilot, (4) contrôleur de vol, (5) chaîne autopilote ESC, (6) moteur, (7) distributeur d'énergie
Effet local	Actionneurs bloqués dans la dernière position commandée
Effet sur système	Maintien du drone sur la dernière position ; (4) mouvement du drone en automatique
Détection	- (1), (2), (3) Pas de réaction du drone aux ordres du pilote (observateur extérieur) ; - (1) Commande erronée en sortie calculateur ; - (3) Données de la liaison non rafraîchies
Action remède	- (1) Basculer sur le redondant (s'il existe) ; - (3) Basculer en mode automatique ; - (2) Basculer dans un mode sûr automatique minimal avec retour au point de départ ou autre point de repli sûr

	préenregistré dans le fichier mission pour un atterrissage automatique

Tableau 4.2: AMDE pour le système de contrôle du drone.

5.4 Mesures de la sûreté de fonctionnement

Le principe de modélisation par le modèle RdPS couplé par des lois de fiabilité, pour calculer les paramètres de la SdF est basé sur les lois de fiabilité selon la nature des composants du système (électronique, mécanique, logiciel, …) où les lois de fiabilité son associé aux places du modèle RdPS placé selon le schéma ci-dessous (***Figure 4.17***) :

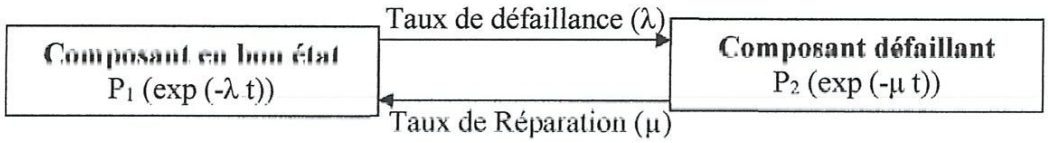

Figure 4.17: Principe de modélisation par le model RdPS couplé par des lois de fiabilité d'un composant défaillant.

Le principe de modélisation d'un composant réparé après défaillance est basé sur le model RdPS couplé avec des lois de fiabilité associe aux places et des taux de défaillance et de réparation associe aux transitions du modèle RdPS comme décrit sur la figure suivant :

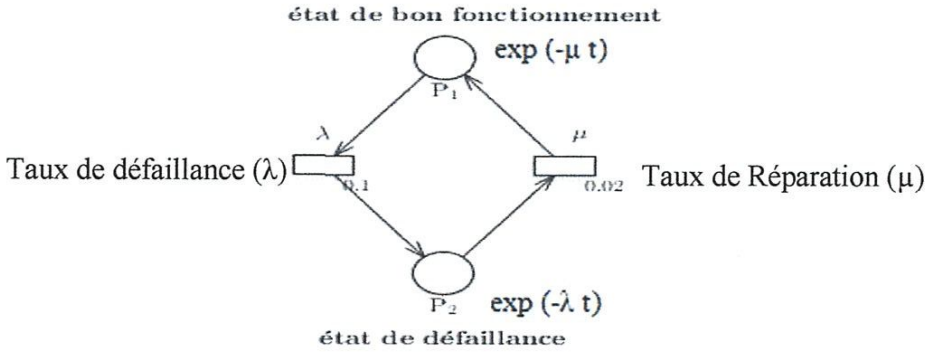

Figure 4.18: Exemple d'un modèle RdPS pour la défaillance et la réparation d'un composant.

L'organigramme de simulation pour l'analyse de la sûreté de fonctionnement d'un système instrumenté de sécurité (SIS), est basé sur le modèle RdPS couplé avec des lois de fiabilité celons la nature des composants (Recueil d'information sur la nature des composants: électriques, mécaniques, électroniques, logiciels,...), pour la génération des scénarios redoutés ainsi que la visualisation des résultats de simulation sur la fiabilité des composants (pour déterminer l'élément le moins fiable), les étapes de l'algorithme sont résumés dans l'organigramme détailler dans la sous-section suivante.

5.5 Organigramme de simulation :

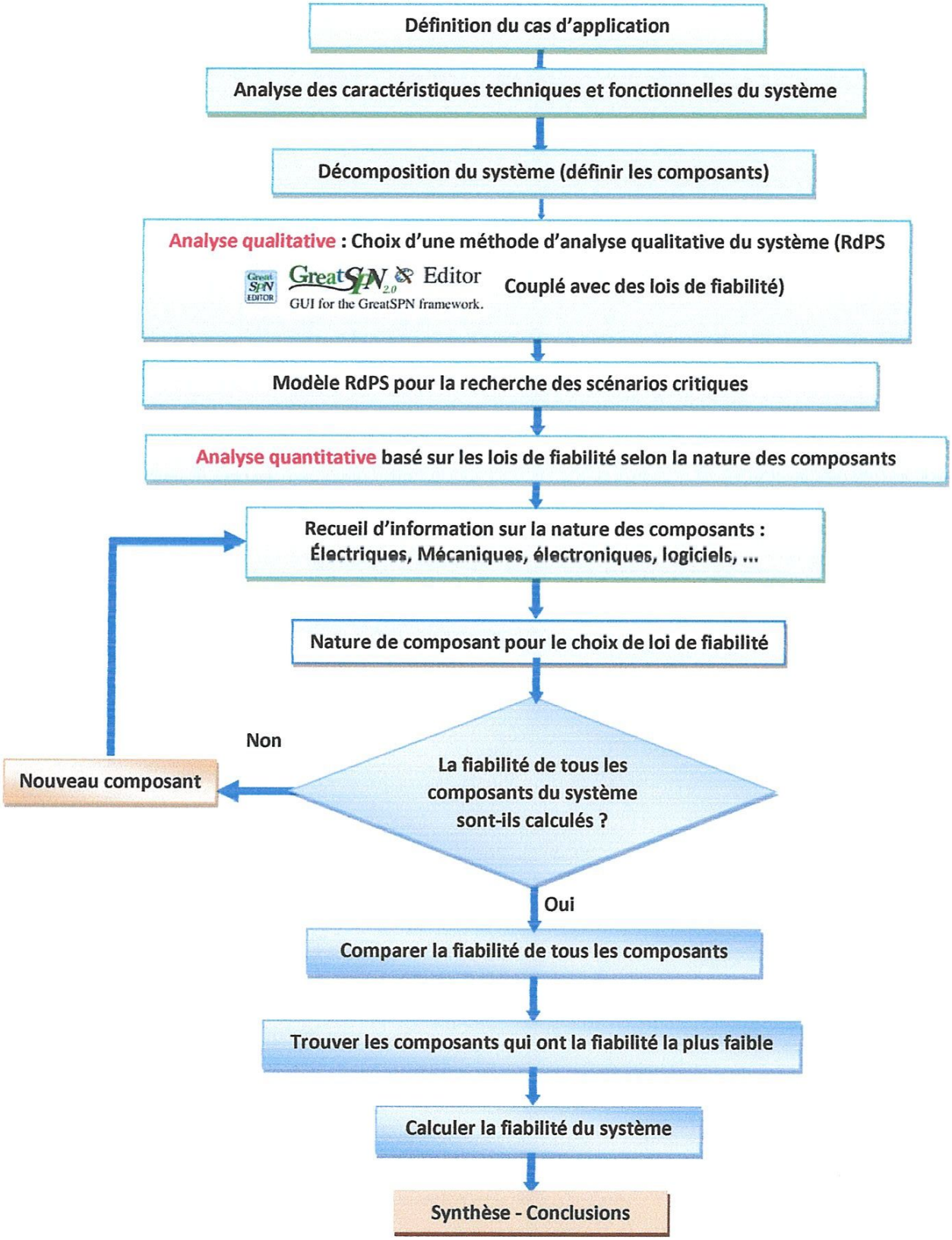

Figure 4.19: Algorithme de simulation

5.6 Modélisation du système étudie par les RdPS sur le logiciel GreatSPN Editor :

Le logiciel de modélisation utilisé pour l'étude de la SdF du cas d'application pour construire le modèle RdPS couplé avec des lois de fiabilité est le logiciel GreatSPN Editor (GSPN), qui permet d'étudié tous les formalismes du modèle RdP (généralisé, déterministe, stochastique, hybride, couplé avec des lois de fiabilité, ...) ainsi que la défaillance des composants :

Figure 4.20 : Logiciel de simulation Great SPN Editor 2.0

Après l'étude du fonctionnement du drone, et à l'aide du logiciel GSPN, on construit le modèle de RdPS globale de notre cas d'application, il est représenté par la ***(Figure 4.21)***

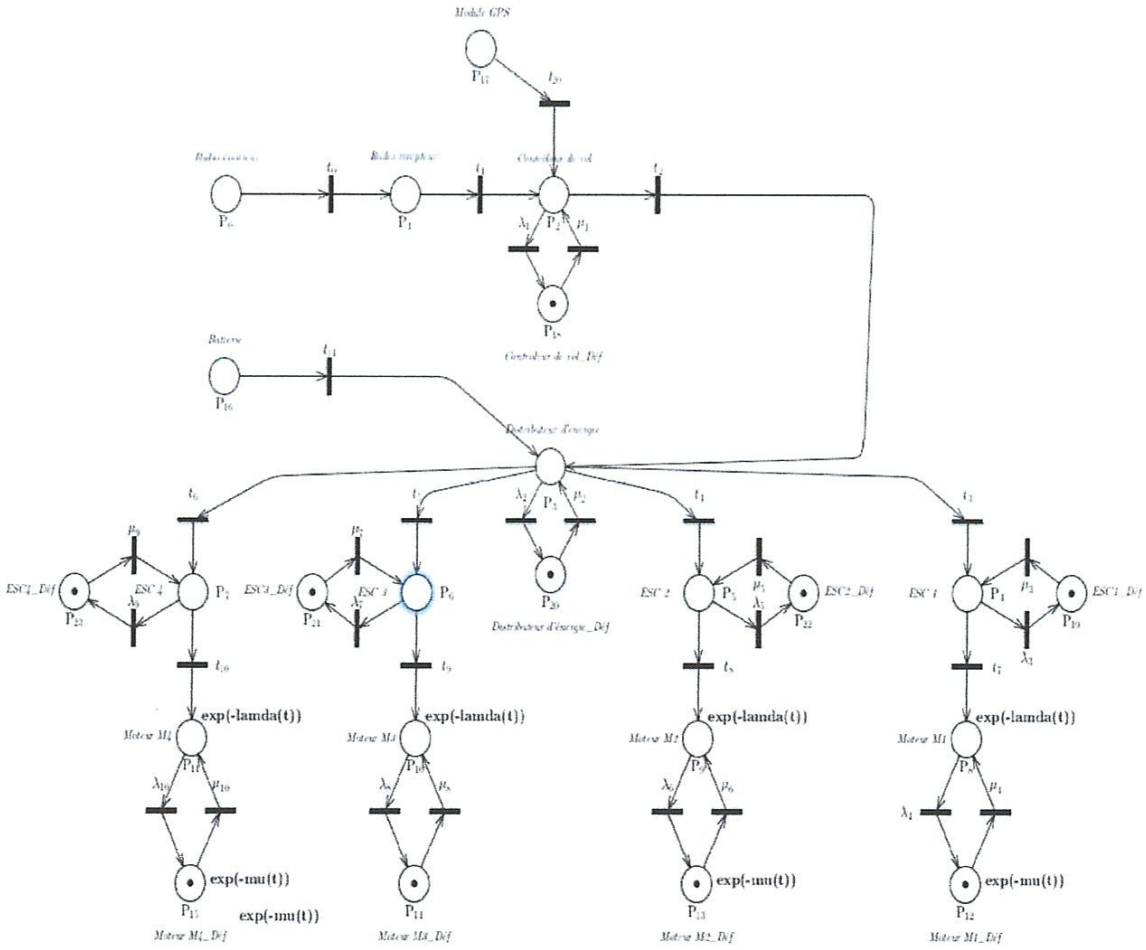

Figure 4.21 : Modèle RdPS global du fonctionnement de drone.

- **Description des places :**

Places de fonctionnement		Places de dysfonctionnement	
Place	**Description**	**Place**	**Description**
P0	Radio émetteur	P12	Moteur M1 Défaillant
P1	Radio récepteur	P13	Moteur M2 Défaillant
P2	Contrôleur de vol	P14	Moteur M3 Défaillant
P3	Distributeur de l'énergie	P15	Moteur M4 Défaillant
P4	Contrôleur de vitesse ESC1	P18	Contrôleur de vol Défaillant
P5	ESC2	P20	Distributeur d'énergie défaillant
P6	ESC3	P19	ESC1 défaillant
P7	ESC4	P21	ESC3 défaillant
P8	Moteur brushless M1	P22	ESC2 défaillant
P9	Moteur M2	P23	ESC4 défaillant
P10	Moteur M3		
P11	Moteur M4		
P16	Batterie		
P17	GPS		

Tableau4.3 : Les places de fonctionnement et de dysfonctionnement

- **Description des transitions :**

Transition	Description
T0	Commande sans fil
T1	Communication électrique
T2	Traitement des informations
T3	Distribution d'énergie
T4	
T5	
T6	
T7	Conversion d'énergie
T8	
T9	
T10	
T11	Alimentation
λ4	Taux de défaillance de M1
μ4	Taux de réparation de M1
λ6	Taux de défaillance de M2
μ6	Taux de réparation de M2
λ8	Taux de défaillance de M3
μ8	Taux de réparation de M3
λ10	Taux de défaillance de M4
μ10	Taux de réparation de M4
T20	Information de localisation
λ1	Taux de défaillance de contrôleur de vol
μ1	Taux de réparation de contrôleur de vol
λ3	Taux de défaillance d'ESC1
μ3	Taux de réparation d'ESC1

- Le scénario redouté 2 trouvé suite à l'exécution du modèle RdP stochastique est :

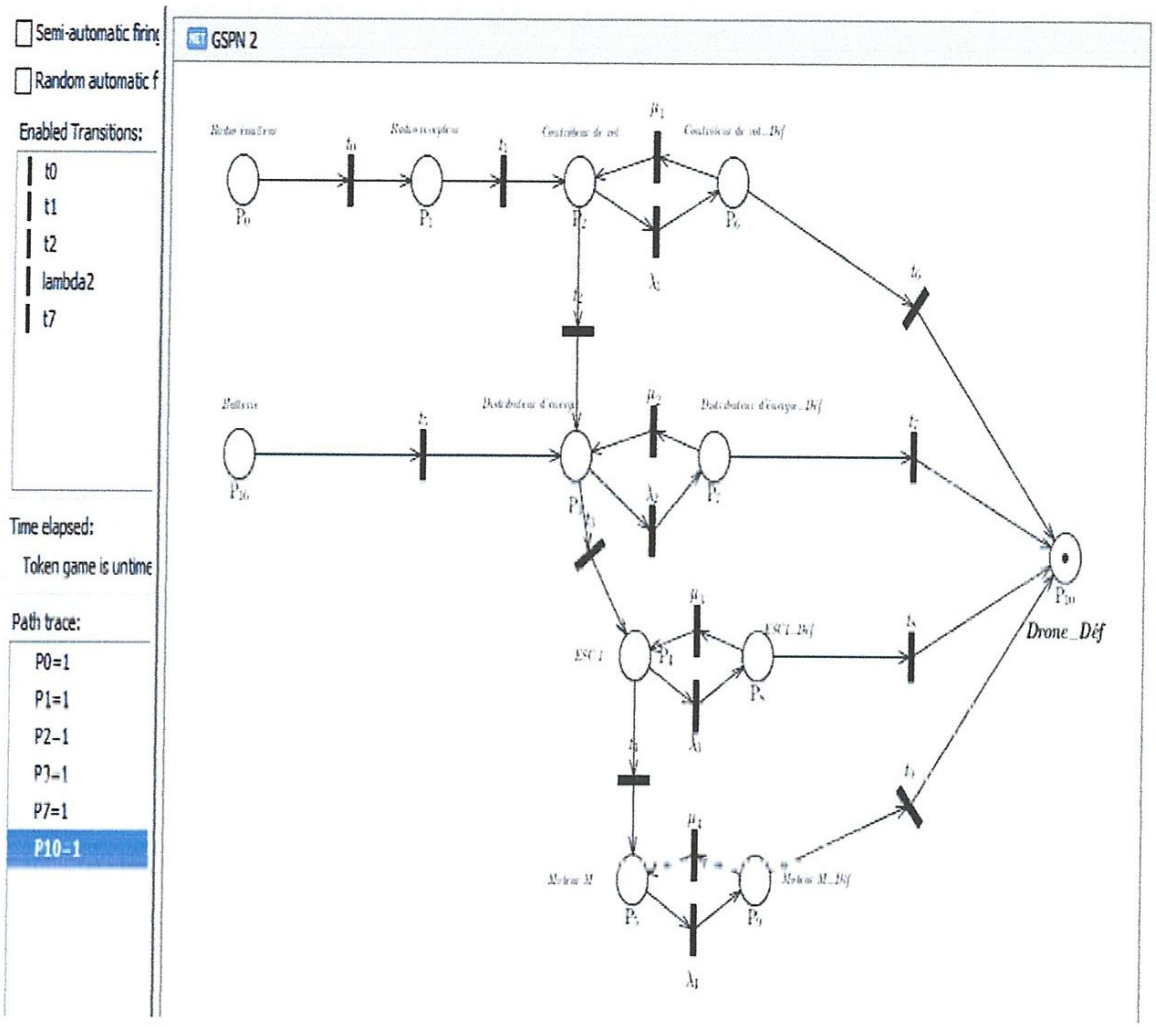

Figure 4.24: Cas ou Distributeur d'énergie est défaillant

A partir de modèle RdP stochastique on trouve le scénario redouté 2 :

$$P0, t0 \rightarrow P1$$

$$P1, t1 \rightarrow P2$$

$$P2, t2 \rightarrow P3$$

$$P3, \lambda 2 \rightarrow P7$$

$$P7, t7 \rightarrow P10$$

Les modes de défaillance sont :

- Aucun moteur ne démarre.
- Un ou plusieurs moteurs ne tournent pas.

- Le scénario redouté 3 trouvé suite à l'exécution du modèle RdP stochastique est :

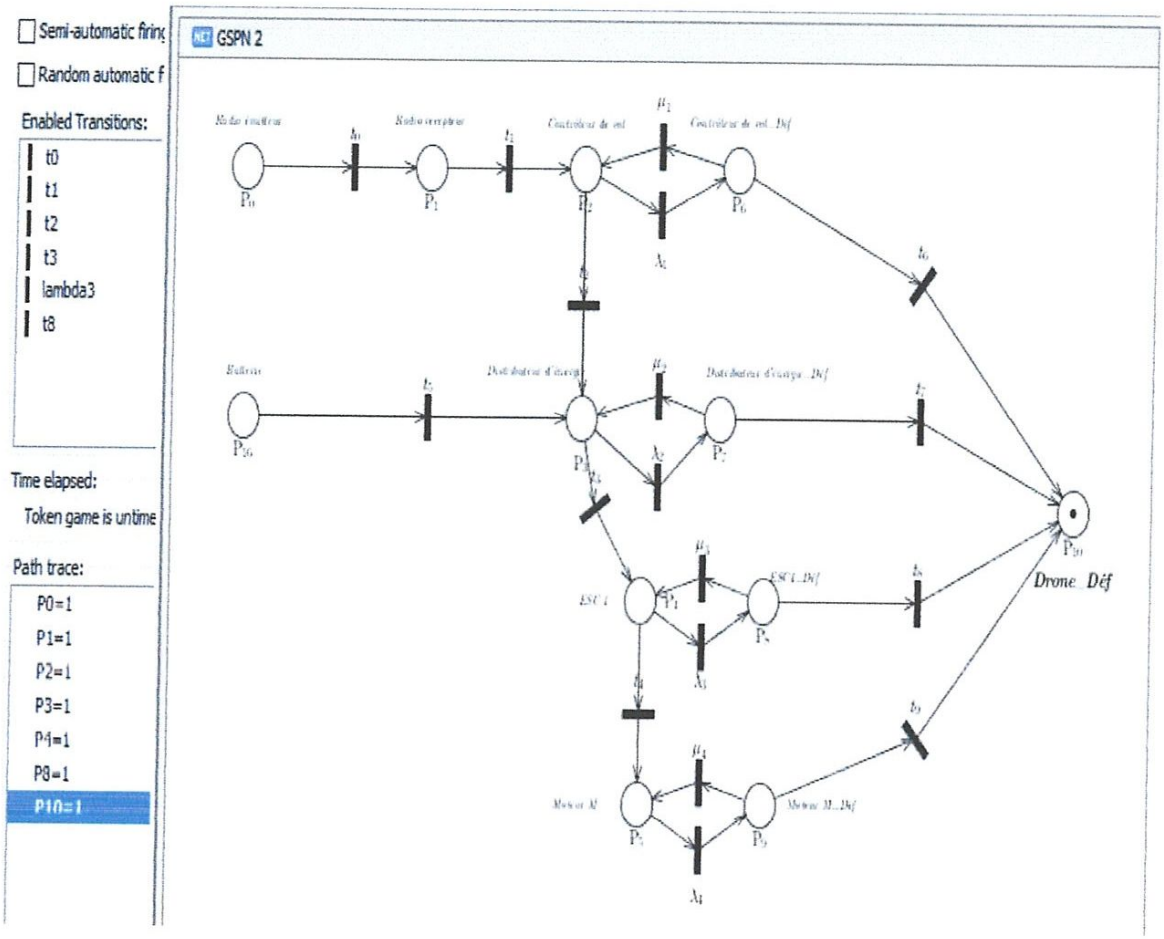

Figure 4.25: Cas ou ESC est défaillant

Scénario redouté 3 :

$$P0, t0 \rightarrow P1$$

$$P1, t1 \rightarrow P2$$

$$P2, t2 \rightarrow P3$$

$$P3, t3 \rightarrow P4$$

$$P4, \lambda 3 \rightarrow P8$$

$$P8, t8 \rightarrow P10$$

Les modes de défaillance trouvée sont :

- Un ou plusieurs moteurs ne tournent pas.
- Moteur obstrué.
- Un moteur tourne dans le mauvais sens.
- Vitesse de tournement de moteur instable.

A partir des résultats obtenus (les scénarios redoutés précédemment détaillées) et après une analyse détaillée, on trouve le scénario redouté global qui mène le système à l'état de la défaillance représenté dans la figure ci-dessous (***Figure 4.27)*** :

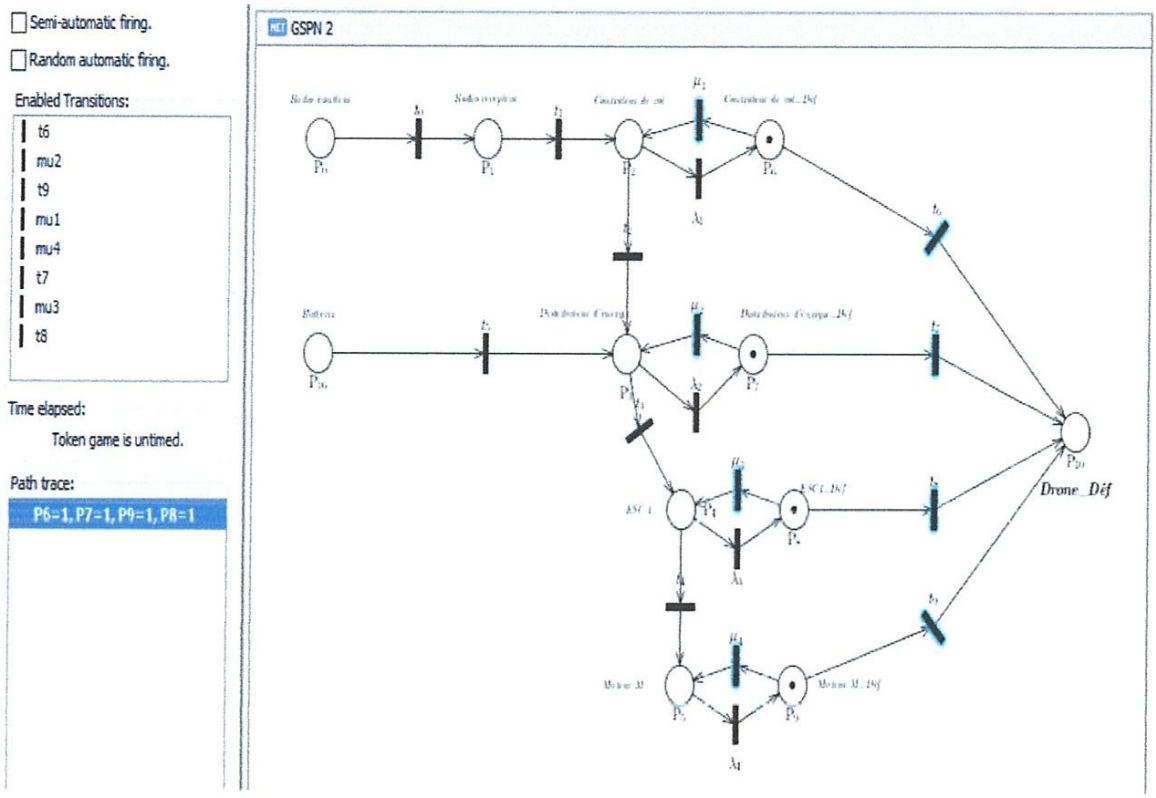

Figure 4.27 Scénario redouté global du système étudié.

Le scénario redouté global qui mène le système à l'état de la défaillance est :

$$P2, \lambda 1 \rightarrow P6$$

$$P3, \lambda 2 \rightarrow P7$$

$$P4, \lambda 3 \rightarrow P8$$

$$P5, \lambda 4 \rightarrow P9.$$

Dans le (***Tableau 4.5***), nous présentons les distributions « dysfonctionnelles » associées aux composants, celons le recueil d'information sur la nature des composants (électriques, mécaniques, électroniques, logiciels, ...) du système étudié.

Conclusion générale

[15] *Mkhida, A. (2008). Contribution μa l'évaluation de la sûreté de fonctionnement des Systèmes Instrumentés de Sécurité intégrant de l'intelligence. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.*

[16] *Rausand, M. and Hoyland, A. (2004). System Reliability Theory ; Models, Statistical Methods and Applications. New York, Wiley, 2nd edition.*

[17] *Rauzy, A., Dutuit, Y., and Signoret, J.-P. (2006). Assessment of safety integrity levels with fault trees. In ESREL Estoril, Portugal.*

[18] *Sallak, M. (2007). Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité. PhD thesis, Nancy Université, Institut National Polytechnique de Lorraine, France.*

[19] *Signoret, J.-P. (2006). Managing risks in hips by making sil calculations effective. In IQPC2006, Aberdeen, Great Britain.*

[20] *Signoret, J.-P., Dutuit, Y., and Rauzy, A. (2007). High integrity protection systems (hips) : Methods and tools for efficient safety integrity levels (sil) analysis and calculations. In Risk, Reliability and Societal Safety Aven and Vinnem (eds).*

[21] *Simon, C., Sallak, M., and Aubry., J.-F. (2007). Sil allocation of sis by aggregation of experts opinions. In ESREL, Safety and Reliability Conference, Stavanger, Norvège.*

[22] *Villemeur, A. (1998). Sûreté de fonctionnement des systèmes industriels. Number 2. Eyrolles.*

[23] *Zhang, T., Long, W., and Sato, Y. (2003). Availability of systems with self-diagnostic components-applying markov model to iec 61508-6. Reliability Engineering Systems Safety, 80 :133141.*

[24] *S. Faucou. Description d'architectures opérationnelles valides temporellement. Thèse de doctorat de l'Institut de Recherche en Communications et en Cybernétique de Nantes (IRCCyN), Décembre 2002.*

[25] *B. Conrard : Contribution à l'évaluation quantitative de la sûreté de fonctionnement des systèmes d'automatisation en phase de conception. Thèse de doctorat. Université Henri Poincaré, Nancy 1, 1999.*

[26] *M. A. Lundteigen. Assessment of hardware safety integrity requirements. Proceedings of the 30th EDReDA Seminar, Trondheim, Norway. June 2006.*

[27] *CEI 62061. Sécurité des machines, sécurité fonctionnelle des systèmes de commande électriques, électroniques et électroniques programmables relatifs à la sécurité. Commission Electrotechnique Internationale, Genève, Suisse, 2005.*

[28] *F. Innal, Y. Dutuit, M. Djebabra. Analyse critique des formules de base de données dans la norme internationale CEI 61508-6. 6ème congrès international pluridisciplinaire, Qualité et sûreté de fonctionnement. Bordeaux, France. Mars, 2005.*

[29] *S. Sklet. Safety barriers: Definitions, classification and performance. Journal of Loss Prevention in the process industries, vol 19, pp 494-506, 2005.*

[30] *E. Fae, J. L. Durka, Conception et évaluation de la sécurité fonctionnelle des systèmes instrumentés de sécurité. Rapport Final, Institut National de l 'Environnement Industriel et des Risques, INERIS, 2000, www.ineris.fr*

[31] J. C. FAGUNDES, *Etude de moteurs à aimants et commutation électronique à champ et courants non sinusoïdaux*, Thèse de doctorat, INPT, 1990.

[32] Rodolphe Jobard, *Les drones, fonctionnement, télé pilotage, application, règlementation. 2éme edition 2016*