République Algérienne Démocratique et Populaire

Ministère de L'Enseignement Supérieur et de la Recherche Scientifique

Université Hadj Lakhdar de Batna

Institut d'Hygiène et Sécurité Industrielle

Laboratoire de Recherche en Prévention Industrielle (LRPI)

Mémoire présenté pour l'obtention du diplôme de:

MAGISTER

en

Hygiène et Sécurité Industrielle

Option: Gestion des risques

Présenté par

M^me^ HADDAD Samia

Ingénieur d'Etat en Hygiène et Sécurité Industrielle

Evaluation et Optimisation des Performances des Systèmes Instrumentés de Sécurité pour une Meilleure Maîtrise des Risques

Soutenue le ……2012.

Devant le Jury

Mr. DJEBABRA Mebarek	*Professeur à l'Université de Batna*	*Président*
Mme BAHMED Lylia	*Professeur à l'Université de Batna*	*Rapporteur*
Mr. INNAL Fares	*Maître de Conférences (A) à l'Université de Batna*	*Co-Rapporteur*
Mr. NAÎT SAÏD Rachid	*Professeur à l'Université de Batna*	*Examinateur*
Mr. SRAIRI Kamel	*Professeur à l'Université de Biskra*	*Examinateur*
Mr. ABDELHADI Bachir	*Maître de Conférences (A) à l'Université de Batna*	*Invité*

2012

A la mémoire de ma défunte mère et à mon cher père

A toute ma petite famille, et particulièrement à Wail

Madame HADDAD SAMIA

Je tiens à exprimer mes sincères remerciements et toute ma gratitude à Madame BAHMED Lylia, Professeure à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté de diriger ce travail, pour son soutien permanent, son aide constante et ses encouragements inconditionnés durant tout ce travail.

Je remercie aussi et profondément Monsieur INNAL Fares, Maître de conférence « A » à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté de co-diriger ce travail avec autant d'efforts, d'attention et de patience jusqu'à son achèvement. Il m'a beaucoup enseigné et aidé à enrichir mes connaissances dans le domaine de la SDF en me donnant des conseils sages et significatifs.

Je présente mes vifs remerciements aux membres du jury de soutenance de ce mémoire de Magister, à savoir :

- ***Monsieur DJEBABRA Mebarek, Professeur à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna, d'avoir accepté de présider le jury de soutenance.***
- ***Messieurs NAIT SAID Rachid, Professeur à l'Institut d'Hygiène et Sécurité Industrielle de l'Université Hadj Lakhdar de Batna et SRAIRI Kamel, Professeur à l'université de Biskra, d'avoir accepté d'évaluer ce travail.***

J'exprime, également, ma profonde gratitude à Monsieur ABDELHADI Bachir, Maître de conférences « A » au Département d'Electrotechnique de l'Université Hadj Lakhdar de Batna pour son aide précieuse et pour ses conseils.

Enfin, je ne dois en aucun cas omettre de remercier Mesdames BOUHIDEL Mouna, KERCHA mabrouka, Chergui Loubna et ma sœur Nawel pour leur orientation et pour leur soutien moral tout le long de la réalisation de ce travail.

Table des matières

Chapitre 2. Probabilités de défaillance dangereuse et sûre (PFD-PFH/PFS-STR)

Chapitre 3. Optimisation des architectures des SIS par les algorithmes génétiques (AG)

Abréviations, acronymes

AdD	Arbre des Défaillances
AG	Algorithmes Génétiques
ALARP	As Low As Raisonably Practicable (aussi faible que raisonnablement possible)
BPCS	Basic Process Control System
CEI	Commission Electrotechnique Internationale (International Electrotechnical Commission)
DC	Diagnostic Coverage (Couverture du Diagnostic)
DCC	Défaillance de Cause Commune
E/E/EP	Electrique / Electronique / Electronique Programmable
EN	European Norm (Norme Européenne)
ER	Evénement Redouté
EUC	Equipment Under Control (équipement à protéger)
GRIF	Graphiques Interactifs pour la Fiabilité
HAZOP	HAZard and Operability study (Analyse de risque et d'exploitation)
IEC	International Electrotechnical Comission
ISA	Instrument Society of America
ISO	International Organisation for Standardization
KooN K	out of N (K parmi N)
LOPA	Layer Of Protection Analysis (Analyse des barrières (couches) de protection)
MDT	Mean Down Time (durée moyenne d'indisponibilité après défaillance)
MTBF	Mean Time Between Failure (durée moyenne entre défaillances consécutives)
MTTF	Mean Time To (first) Failure (durée moyenne de fonctionnement avant la Première défaillance)
MTTR	Mean Time To Repair (durée moyenne de réparation)
MUT	Mean Up Time (durée moyenne de fonctionnement après réparation)
NF	Norme Française
PFD	Probability of Failure on Demand (probabilité de défaillance à la demande)
PFH	Probability of Failure per Hour (probabilité de défaillance par heure)
PFS	Probabilité de défaillance sûre (Intempestif)
RFF	Risk Reduction Factor (facteur de réduction du risque)
SFF	Safe Failure Fraction (proportion des défaillances en sécurité)
SIF	Safety Instrumented Function (fonction instrumentée de sécurité)
SIL	Safety Integrity Level (niveau d'intégrité de sécurité)
SIS	Safety Instrumented System (Système Instrumenté de Sécurité).
SRS	systèmes relatifs a la sécurité (safety related systems)
STR	le taux de défaillance sûr(Intempestif)

Liste des figures

Liste des tableaux

Introduction

1. Problématique

Les démarches de maîtrise des risques visent en priorité à réduire le risque existant, inhérent à une application donnée, à un niveau jugé tolérable et à le maintenir dans le temps. Cette réduction est souvent obtenue par l'interposition successive de plusieurs barrières de protection entre la source de danger, qui peut être un procédé industriel, et les cibles potentielles que sont les personnes, les biens et l'environnement. Ces barrières incorporent souvent des systèmes instrumentés de sécurité (*SIS : Safety Instrumented System)*. L'objectif premier assigné à ce type de systèmes est la détection des situations dangereuses (augmentation de température ou de pression, fuite de gaz…) pouvant mener a un accident (incendie, explosion, rejet d'un produit dangereux...) et de mettre ensuite en œuvre un ensemble de réactions nécessaires a la mise en sécurité de l'équipement à protéger (*EUC : Equipment Under Control*).

Vérifier l'aptitude du *SIS* à exécuter correctement ses fonctions constitue une étape combien importante pour la validation de ce dernier. A ce titre plusieurs documents normatifs ont été élaborés afin de guider les fabricants et utilisateurs potentiels des *SIS* dans leur démarche de validation. Parmi celles-ci, la norme CEI 61508 représente le document normatif central pour la conception et l'exploitation des *SIS* [CEI 61508]. Elle met en œuvre, en tant que cadre technique, un modèle de cycle de vie de sécurité global et adopte le concept de niveau d'intégrité de sécurité (*SIL : Safety Integrity Level*) qui spécifie les exigences (qualitatives et quantitatives) sur la fonction de sécurité implémentée au niveau du *SIS*. Les exigences quantitatives d'intégrité de sécurité (intégrité de sécurité du matériel) doivent être traduites en mesures cibles de défaillances. Ces dernières s'identifient à la probabilité moyenne de défaillance à la demande du *SIS* (*PFD_{moy} : Probability of Failure on Demand*) pour un *SIS* fonctionnant en « *faible demande* », et à sa probabilité de défaillance dangereuse par heure *(PFH* : *Probability of Failure per Hour*) s'il est appelé à fonctionner en mode « *demande élevée ou continue* ».

Si assurer la sécurité des installations et la sauvegarde de leur environnement, notamment humain, est l'objectif premier affiché de la norme CEI 61508, elle ne spécifie cependant aucunes exigences liées aux activations intempestives des *SIS* [INNAL, 2008]. En effet, la qualité de service d'une fonction instrumentée dédiée à la sécurité (*SIF : Safety Instrumented Function)* correspond à la propriété de satisfaire à la fois le *SIL* établi au cours de l'analyse de risques (performance définie par la CEI 61508 : *PFD_{moy} ou PFH)* et les objectifs de production (non perturbation de la mission du système (*EUC*) en absence de situation dangereuse). Evidemment, si les arrêts d'urgence intempestifs sur une installation donnée sont trop fréquents, ils se révèlent économiquement préjudiciable, voire dangereux.

Donc, le comportement attendu d'un *SIS* est double :

- Activer la fonction de sécurité en cas d'occurrence de la demande (***intégrité de sécurité***).
- ne pas activer la fonction de sécurité en absence de la demande (***intégrité opérationnelle***).

Par ailleurs, ces deux grandeurs (intégrités de sécurité et opérationnelle) peuvent être antagonistes. Ainsi, tenter d'augmenter l'intégrité de sécurité, en réduisant la probabilité de défaillance dangereuse du *SIS*, peut aussi diminuer significativement son intégrité opérationnelle par l'augmentation des déclenchements intempestifs (la réciproque est vraie). La meilleur politique à entreprendre, pour concevoir un *SIS* performant, est celle de compromis optimal entre son intégrité de sécurité et son intégrité opérationnelle. Etablir les bases d'une telle politique est la principale ambition de ce mémoire de magistère.

2. Objectifs

Comme explicité précédemment, la conception des *SIS* assurant une double performance, satisfaire aux objectifs de sécurité et de disponibilité, constitue une tâche d'importance capitale.

Dans cette optique, l'objectif de ce travail de recherche est d'abord de proposer une formulation analytique des performances des *SIS*, au regard des objectifs de sécurité et de disponibilité, et d'établir ensuite quelques réflexions en rapport avec l'optimisation des architectures des *SIS*. Cette proposition s'inscrit donc des domaines d'application aussi divers que l'analyse des risques et aide à la décision, l'étude probabiliste des risques, l'optimisation des performances et réduction des coûts, etc.

En effet, afin d'optimiser l'architecture d'un *SIS*, il est nécessaire dans un premier temps de définir sans ambigüité l'ensemble des grandeurs qui y contribuent. A cet effet, et en relation avec le contexte de l'étude proposée, nous avons retenu les indicateurs de performance suivants :

- *Indicateurs d'intégrité de sécurité :* la probabilité moyenne de défaillance à la demande du *SIS* (PFD_{moy}) et sa probabilité de défaillance dangereuse par heure (*PFH*).
- *Indicateurs d'intégrité opérationnelle.* A l'image des deux indicateurs précédents, les deux indicateurs suivants sont les plus significatifs vis-à-vis de la disponibilité de production des procédés industriels : la probabilité moyenne de défaillance en sécurité (PFS_{moy} *: Probability of Failing Safely*) et le taux de déclenchement intempestif (*STR : Spurious Trip Rate*). Comme la CEI 61508 est orientée sécurité, ces deux derniers indicateurs n'y sont pas abordés.

Pour ces quatre indicateurs nous effectuerons une étude bibliographique afin d'analyser les différentes formulations analytiques existantes. Ensuite, nous proposerons une démarche, fondée sur la modélisation des architectures système *KooN* (le système fonctionne si au moins *K* composants fonctionnent parmi les *N*) via les chaînes de Markov, permettant d'établir les formules analytiques des PFS_{moy} et *STR* de ces architectures. Nous signalons que cette même démarche a permis d'obtenir, dans une étude précédente [INNAL, 2008] les formules analytiques relatives aux PFD_{moy} et *PFH*.

Nous aborderons finalement le problème d'optimisation par une démarche basée sur les algorithmes génétiques (*AG*). Sans vouloir anticiper les choses, un *AG* est un algorithme itératif de recherche d'optimum qui copie de façon extrêmement simplifiée certains comportements des populations naturelles. Ainsi, un *AG* repose sur l'évolution d'une population de solutions qui sous l'action de règles précises (sélection, croisement et mutation) optimise un comportement donné, exprimé sous forme d'une fonction dite fonction objective. Au cours de cette dernière partie, l'optimisation d'un *SIS* sera traitée selon de différentes stratégies.

3. Organisation du mémoire

Le présent mémoire est scindé en trois chapitres :

- Au niveau du ***premier chapitre*** seront présentés, dans un premier temps, quelques concepts et définitions liés à la démarche d'analyse des risques. Nous évoquerons ensuite l'organisation de la norme CEI 61508 qui constitue, rappelons-le, le document de référence pour la mise en œuvre des *SIS*. Enfin, nous définirons les systèmes instrumentés de sécurité et donnerons leur organisation et leur fonctionnement.

- Le ***deuxième chapitre*** est d'abord consacré à une étude bibliographique ayant pour objet d'établir un état de l'art relatif aux formulations mathématiques des indicateurs de performance retenus dans le cadre de ce mémoire (PFD_{moy}, *PFH*, PFS_{moy}, *STR*). Nous présentons un échantillon de résultats les concernant en vue d'une comparaison simplifiée des différentes approches recensées. La dernière partie de ce chapitre s'inscrit dans la continuité de l'étude bibliographique précédente. Son objectif est de vérifier l'adéquation des formulations analytiques existantes ayant trait à la PFS_{moy} et le *STR*. Pour ce faire, nous proposons une nouvelle formulation mathématique en mettant à profit les chaînes de Markov qui permettent une modélisation comportementale effective des systèmes testés périodiquement.

- Une approche d'optimisation des *SIS* sera détaillée au cours du ***troisième et dernier chapitre.*** Nous explicitons d'abord le problème d'optimisation en exposant les différents facteurs et critères rentrant en ligne de compte. Pour simplifier l'appréhension, ceci sera réalisé au travers d'un exemple réaliste issu de l'industrie de procédés. Sera ensuite décrite la démarche d'optimisation adoptée : les algorithmes génétiques (*AG*). Nous l'appliquerons finalement à notre exemple illustratif. A ce titre, plusieurs stratégies de maintenance seront testées, allant d'une stratégie simpliste (minimisation de la PFD_{moy} sans aucunes contraintes) à une stratégie plus complète (optimisation multi-objectifs).

In fine ce mémoire sera clos par une conclusion générale résumant le travail réalisé et donnant les perspectives de recherche envisagées.

CHAPITRE 1

De la gestion des risques aux systèmes instrumentés de sécurité

1.1. Introduction

Les industriels ne se préoccupent plus uniquement des performances des systèmes en termes de qualité, de productivité et de rentabilité mais aussi en termes de sécurité [TIENNTO *et al*., 2008]. A ce titre, la maîtrise des risques industriels leurs impose de mener des analyses de risques dans le but d'identifier les scénarios d'accidents susceptibles de se produire au niveau de leurs installations et qui constituent des sources de dommage pour les personnes, les bien et l'environnement. Quelque soit la méthodologie d'analyse retenue, ces analyses ont pour vocation première de s'assurer que les mesures de maîtrise des risques (*MMR*) mises en place permettent d'amener le niveau de sécurité de l'installation à l'objectif recherché [IDDIR, 2009].

Pour que cette assurance soit vérifiée, les actions entreprises doivent être inscrites dans un processus de gestion des risques capable d'identifier, de mesure et de maîtriser les risques d'une manière effective. C'est dans cette optique que la norme CEI 61508 à été développée. Son objectif affiché est la mise en place des systèmes (barrières, mesures, couches) de sécurité de type instrumenté en fonction de la réduction nécessaire du risque.

Dans ce chapitre, nous allons d'abord donner quelques concepts et définitions liés à la gestion des risques et décrire le processus de gestion des risques, avant d'exposer l'essentiel de la CEI 61508 de même que les *SIS* qui constituent l'objet premier de ce travail de recherche.

1.2. Concepts et définitions

1.2.1. Notion de système

Le mot système constitue un concept capital, car il souligne l'importance des liaisons existantes entre les variables qui définissent une situation donnée. Système dérive du grec « systema » qui signifie « ensemble organisé » [CEA, 2002]. Plusieurs définitions ont été proposées pour le mot système. Nous nous limitons cependant à celle proposée par J. L. Le Moigne [LE MOIGNE, 1984], qui considère un système comme : « *un objet doté de finalité qui, dans un environnement, exerce une activité et voit sa structure interne évoluer au fil du temps, sans qu'il perde pourtant son identité* ». D'une manière générale, un système peut être vu comme :

- quelque chose (n'importe quoi présumé identifiable),
- qui fait quelque chose (activité, fonctionnement),
- dans quelque chose (environnement),
- pour quelque chose (finalité, projet),
- par quelque chose (structure = support de l'activité),
- et qui se transforme dans le temps (évolution).

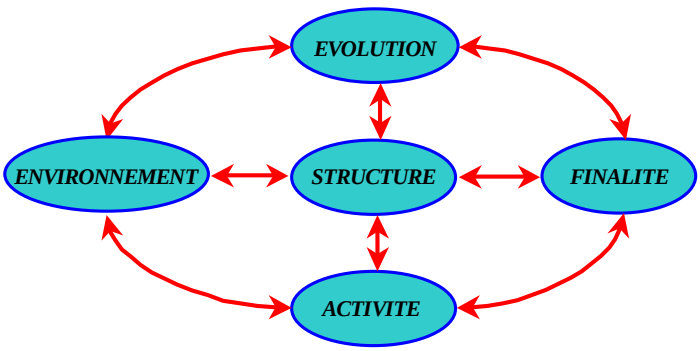

Figure 1.1 : Les attributs du mot système

1.2.2. Notion de danger

Selon la norme CEI 61508 et la référence [DESROCHES, 1995], *le danger désigne une nuisance potentielle pouvant porter atteinte aux biens (détérioration ou destruction), à l'environnement, ou aux personnes. Les dangers peuvent avoir une incidence directe sur les personnes, par des blessures physiques ou des troubles de la santé, ou indirecte, au travers de dégâts subis par les biens ou l'environnement.*

Le référentiel OHSAS 18001 [OHSAS, 1999] définit un danger comme suit : *une source ou une situation pouvant nuire par blessure ou atteinte à la santé, dommage à la propriété et à l'environnement du lieu de travail ou une combinaison de ces éléments.*

La définition du mot danger que proposait la 3SF [3SF, 1974] pour un système donné : « *Le danger inhérent à un système est défini par le répertoire (la liste) des événements redoutés qu'il est susceptible d'engendrer* ». La nature qualitative et descriptive du danger apparaît clairement dans cette définition.

1.2.3. Notion de risque

Le risque tient compte d'une exposition un danger. Pour bien apprécier les effets négatifs d'un dommage potentiel lié à un danger, une autre dimension est à considérer : combien de fois ce dommage peut se produire. Cette idée nous amène à la notion du risque. Le risque peut être vu donc comme la possibilité qu'un danger s'actualise, c'est-à-dire entraîne effectivement des dommages. Le terme possibilité est généralement formalisé sous forme de probabilité ou de fréquence. Le risque peut donc être considéré comme une certaine quantification du danger associant une mesure de l'occurrence (probabilité ou fréquence) d'un événement redouté à une estimation de la gravité de ses conséquences. Ainsi, bien qu'il existe de nombreuses définitions pour caractériser le sens du mot risque, la définition suivante est celle que l'on rencontre souvent : *« la combinaison de la probabilité d'occurrence d'un dommage et la gravité de ce dernier »* [ISO, 1999].

Le terme combinaison est généralement matérialisé par une opération de multiplication, se qui nous permet la formulation suivante : *Risque* (*R*) = *Probabilité* (*P*) × *Gravité* (*G*). La représentation graphique de cette relation est une droite ou une courbe décroissante. Elle dérive de la courbe dite de *Farmer* [LIEVENS, 1976] et permet d'illustrer la partition de l'espace du risque en deux sous-ensembles disjoints, correspondant respectivement au domaine du risque acceptable et à celui du risque inacceptable (figure 1.2).

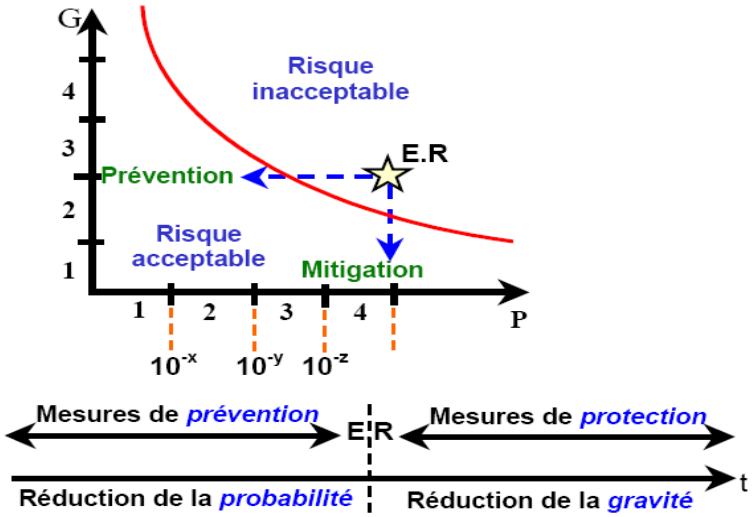

Figure 1.2 : L'espace du risque

La figure suivante permet de bien apprécier l'interaction entre les notions de danger et de risque (émergence de la notion de situation dangereuse).

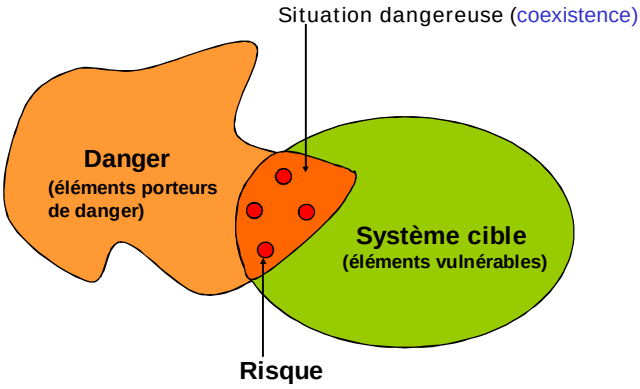

Figure 1.3 : Relation entre les notions de danger et de risque

1.2.4. Notion de sécurité

La sécurité peut être vue comme la tranquillité d'esprit inspirée par la confiance, par le sentiment de n'être pas menacé. Elle est en général associée à l'absence de risque inacceptable. A ce titre et en suivant le guide ISO/CEI 73 [ISO, 2002], la sécurité est *l'absence de risque inacceptable, de blessure ou d'atteinte à la santé des personnes, directement ou indirectement, résultant d'un dommage au matériel ou à l'environnement.*

A l'instar de ce qui est fait pour la fiabilité et la disponibilité dans diverses normes, la sécurité d'un système peut être définie en termes d'aptitude : « *la sécurité d'un système est son aptitude à fonctionner ou à dysfonctionner sans engendrer d'événement redouté à l'encontre de lui même et de son environnement, notamment humain* » [INNAL, 2008].

Connaître ses risques constitue une préoccupation permanente des entreprises et de leurs dirigeants. Mettre en place un dispositif de gestion des risques qui permettra de les maîtriser et donc d'assurer la sécurité des cibles potentielles est désormais, comme nous l'avons signalé, un de leurs objectifs prioritaires. L'objet de la section suivante est de donner les lignes directrices du processus de maîtrise des risques.

1.3. La gestion des risques

La gestion des risques est l'un des enjeux majeurs de toute activité industrielle. Elle doit faire partie de la politique globale de l'entreprise et constitue par là l'une des composantes fondamentales de sa réussite. Aujourd'hui il incombe à tout exploitant de démontrer qu'il gère aux mieux les risques générés par son installation par la mise en place des mesures nécessaires permettant d'assurer la sécurité des personnes, des biens et de l'environnement.

La gestion des risques peut être définie comme *l'ensemble des activités coordonnées en vue de réduire le risque à un niveau jugé tolérable ou acceptable*. Cette gestion constitue un processus itératif qui englobe de différentes phases dont l'enchaînement est décrit à la figure 1.4 [INERIS, 2003].

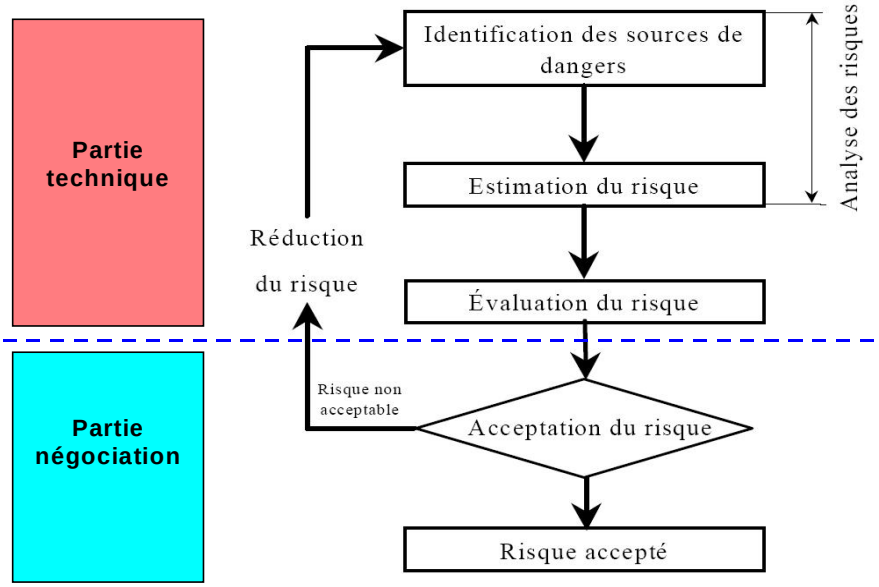

Figure 1.4 : Processus de gestion des risques

Ces différentes phases sont brièvement explicitées comme suit.

1.3.1. Analyse des risques

L'analyse des risques est définie dans le Guide ISO/CEI 51 [ISO, 1999] comme : « *l'utilisation des informations disponibles pour identifier les phénomènes dangereux et estimer le risque* ». Cette phase se compose des points suivants :

- La première étape d'une démarche de gestion des risques consiste en l'identification, le plus exhaustivement possible, de l'ensemble des sources de dangers et des scénarios associés qui peuvent entraîner des dommages. Ceci est possible une fois que le système à étudié est identifié et le domaine de l'étude (surtout en termes d'objectif de sécurité) est déterminé sans ambiguïté.
- Consécutivement à cette identification, l'estimation de chaque scénario d'accident doit considérer les deux composantes du risque :
  - la probabilité (ou fréquence) d'occurrence,
  - Les conséquences potentielles associées.

Cette estimation peut être réalisée à l'aide de méthodes telles que : APR, HAZOP, AMDEC, AdD, …) ; prises individuellement ou combinées. Notons également que cette phase, comme les autres phases, est conduite par un groupe de travail multidisciplinaire dont l'expertise conditionne considérablement la qualité et l'efficacité de la démarche de gestion des risques.

1.3.2. Evaluation des risques

Cette phase permet de situer le travail d'analyse par rapport aux objectifs fixés. Elle revient à comparer le niveau de risque estimé à celui jugé acceptable ou tolérable. L'acceptation du risque et une étape de négociation entre les différents partenaires impliqués dans la démarche de gestion des risques. Bien évidement, les critères d'acceptabilité du risque doivent résulter d'un consensus entre ces partenaires.

1.3.3. Réduction du risque

La réduction du risque doit être considérée dès lors que le risque considéré est jugé inacceptable. Il s'agit d'identifier les barrières nécessaires pour ramener le niveau de risque des différents scénarios d'accidents, en agissant le plus en amont possible de leur développement (principe d'élimination à la source), à un niveau acceptable. Comme nous l'avons précisé, rappelons-le, le risque est une combinaison de la probabilité d'un événement dangereux et de sa gravité. Ceci étant, la réduction du risque peut être obtenue de deux manières différentes (figure 1.2) :

- ***La protection :*** elle regroupe les mesures prises pour limiter les conséquences de la survenue d'un accident en diminuant ainsi sa gravité. Par exemple : une cuvette de rétention assurant le non épandage d'un liquide, un système d'extinction automatique permettant de réduire les effets d'un incendie, les plans de secours et les procédures d'urgence pouvant réduire largement les dommages susceptibles d'être occasionnés, etc.
- ***La prévention :*** elle a pour but la réduction de sa probabilité (ou fréquence) d'occurrence. La prévention désigne donc les mesures préalables mises en place pour empêcher la survenue d'un accident. Cela peut être assuré par une conception sûre de l'installation ou par l'ajout de systèmes assurant la sécurité de l'installation en cas de dérive. Ainsi, pour protéger une installation contre les surpressions, les mesures de prévention peuvent consister en une soupape de sécurité, un disque de rupture ou encore en un système automatique d'arrêt d'urgence (*SIS*).

L'aptitude de réduction du risque des barrières proposées, ou même existantes, doit être évaluée et maintenu dans le temps, d'où l'intérêt de la CEI 61508 et ses normes filles dans le cadre des barrières basées sur une technologie instrumentée.

Par ailleurs, les risques assumés, résiduels, doivent être contrôlés et gérés notamment par :

- La sensibilisation et la communication sur ces risques. A ce titre, les exploitants sont tenus pour responsables et sont suspectés s'ils n'ont pas communiqué de manière suffisamment transparente sur les risques qui dépendent de leur autorité.
- Le maintien et le contrôle des mesures de réduction mises en place.
- La gestion financière et assurances.

Il convient de noter qu'il existe plusieurs cadres génériques définissant la structure générale d'un système de mangement des risques ou de sécurité. Nous citons, à titre d'exemple : OHSAS 18001 [OHSAS, 1999], ILO-OSH 2001 (développé par le Bureau International du Travail (BIT)) [ILO-OSH, 2001] et l'ISO 31000 [ISO 31000, 2009].

1.4. Norme CEI 61508 et processus de gestion des risques

Si l'instrumentation doit réellement être utilisée pour réaliser des fonctions instrumentées de sécurité, il est essentiel qu'elle présente des niveaux minimums de qualité et de performance. En conséquence, un grand travail a été effectué mettant en question les performances des systèmes relatifs à la sécurité de type instrumenté, considérés comme complexes, par le développement des normes qui favorisent l'évaluation, la validation et la certification systématique de ces systèmes. Parmi ces différents documents normatifs, la norme CEI 61508 développée et publiée par la Commission d'Electrotechnique Internationale (CEI), intitulée *«Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité»*, occupe une place incontournable dans la maîtrise des risques par des systèmes instrumentés. Nous donnons, dans la suite de cette section, les différents éléments-clés permettant de saisir la démarche de maîtrise des risques préconisée par la CEI 61508.

1.4.1. Norme CEI 61508

La norme CEI 61508, constituée de sept parties (voir annexe 1 pour le résumé de chaque partie), est développée comme norme générique qui contient un ensemble d'informations et lignes directives concernant l'amélioration de la sécurité à travers l'utilisation des systèmes de sécurités instrumentés (*SIS*). Elle s'inscrive dans une approche globalisée de la sécurité que l'on pourrait comparer au système ISO 9000 pour la qualité, et au système ISO 14000 pour l'environnement. L'un des principaux objectifs de la CEI 61508 est d'être utilisé par les organisations internationales de normalisation comme une base pour le développement des normes spécifiques à chaque secteur d'application (voir figure 1.5). Elle permet donc d'avoir des principes et langages communs.

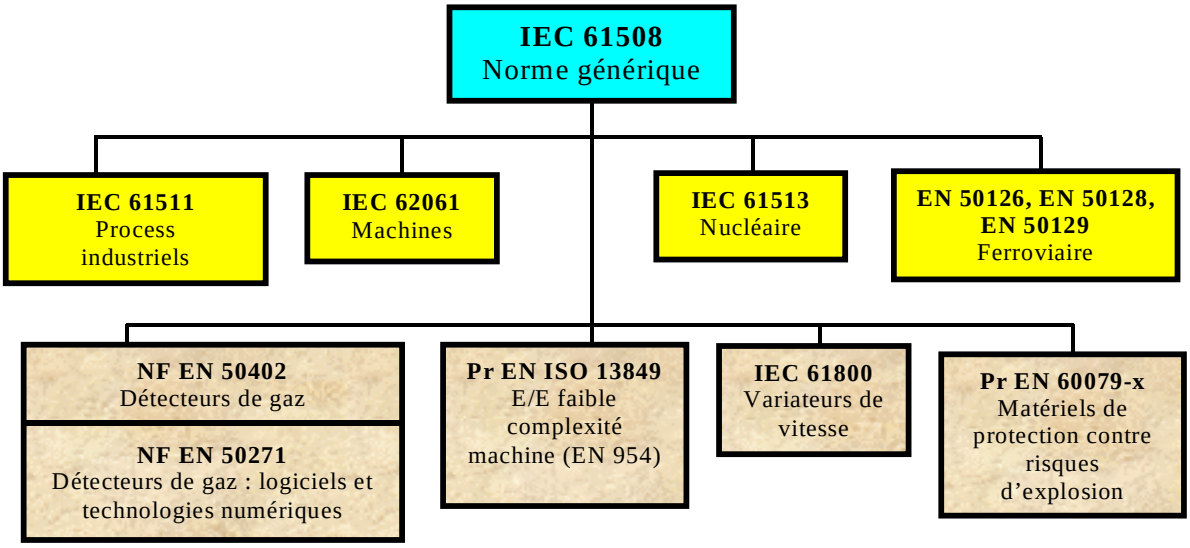

Figure 1.5 : CEI 61508 et ses déclinaisons par secteur d'application

Le principe fédérateur de cette norme est fondé sur le modèle de *cycle de vie globale de sécurité*, depuis la spécification, en passant par la conception, l'installation, l'exploitation et la maintenance, jusqu'à la mise hors service des *SIS*, comme montré à la figure 1.6. Le cycle de vie fournit un guide complet pour l'établissement des caractéristiques et spécifications relatives aux fonctions de sécurité allouées aux *SIS*.

Globalement, trois grandes parties dans le cycle de vie global de sécurité peuvent être distinguées :

- Les premières étapes se basent sur une *analyse de risques* pendant laquelle l'ensemble des situations dangereuses (scénarios d'accident) est établi, en termes de gravité et de probabilité (fréquence) d'occurrence, afin d'en comparer la criticité à une valeur limite constituant l'objectif de sécurité à atteindre. Si cette criticité excède la valeur-seuil précitée, il sera alors nécessaire de la réduire. L'ampleur de cette réduction donne lieu à la définition de prescriptions globales de sécurité (phase 4) en termes de fonctions de sécurité et de prescriptions d'intégrité de sécurité (voir la définition de cette notion plus bas dans ce document) qui sont ensuite déclinées en prescriptions particulières de sécurité (phase 5) allouées aux différents moyens de réduction de risques (voir figure 1.7). Pour les *SIS*, ces prescriptions sont établies en termes de niveaux d'intégrité de sécurité (*SIL requis*) (voir figure 1.8). Plus la réduction de risque à réaliser est importante, plus le *SIL* est élevé. Ce constat souligne l'importance et le rôle capital que joue l'analyse de risques dans l'ensemble

du cycle de vie. Nous allons plus loin donner quelques méthodes de détermination du *SIL* requis, telles décrites dans les références [CEI 61508-5, 2000] et [CEI 61511-1, 2003].

- Puis vient le cycle de vie inhérent au développement des moyens de réduction de risques (SIS, systèmes relatifs à la sécurité basés sur d'autres technologies, moyens externes de réduction de risques) : phases 9, 10 et 11 (voir la figure 1). Comme nous l'avons déjà noté, la CEI 61508 ne considère que les spécifications relatives au développement des systèmes instrumentés de sécurité (phase 9).
- Ces deux premières parties sont complétées par les phases d'installation et de validation globale de la sécurité, de fonctionnement et de modifications éventuelles, avec, le cas échéant, un retour à la phase adéquate du cycle de vie.

Il convient de noter que CEI 61508 recommande l'adoption et la mise en application du cycle de vie de sécurité dans le système de management de la sécurité (*SMS*) de l'établissement concerné.

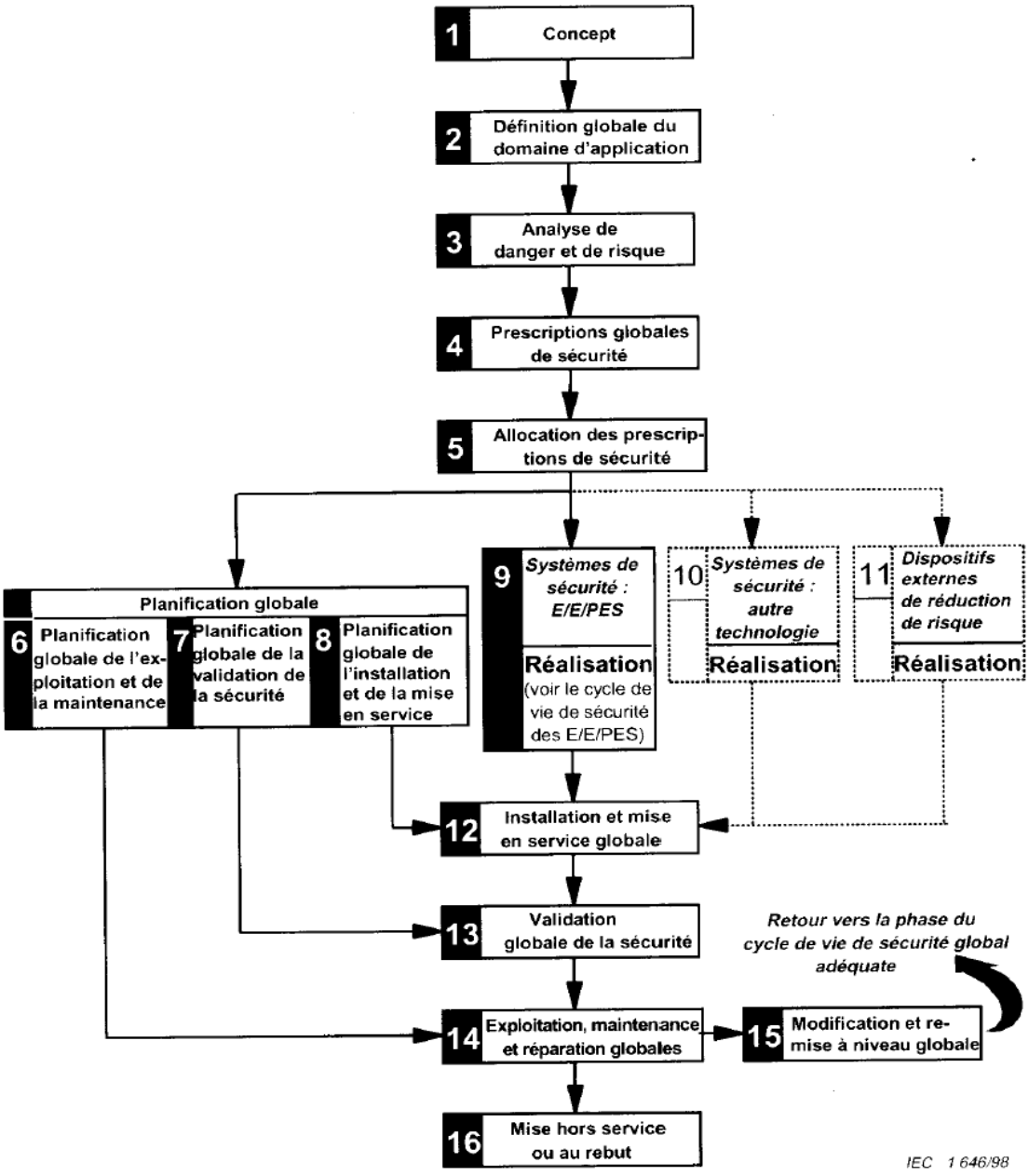

Figure 1.6 : Cycle de vie de sécurité globale [IEC 61508-1]

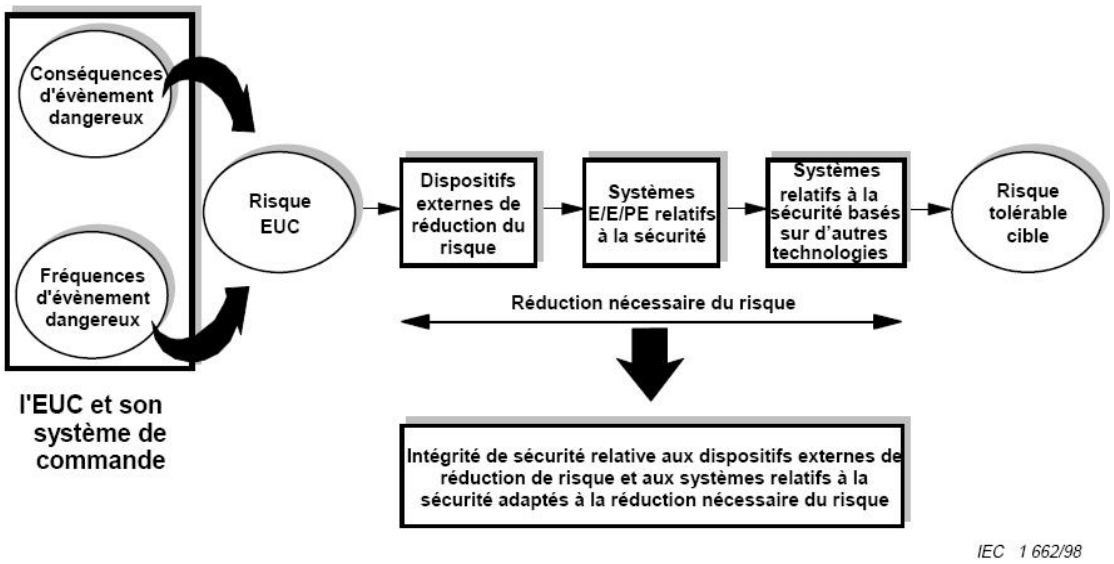

Figure 1.7 : Concept de risque et d'intégrité de sécurité

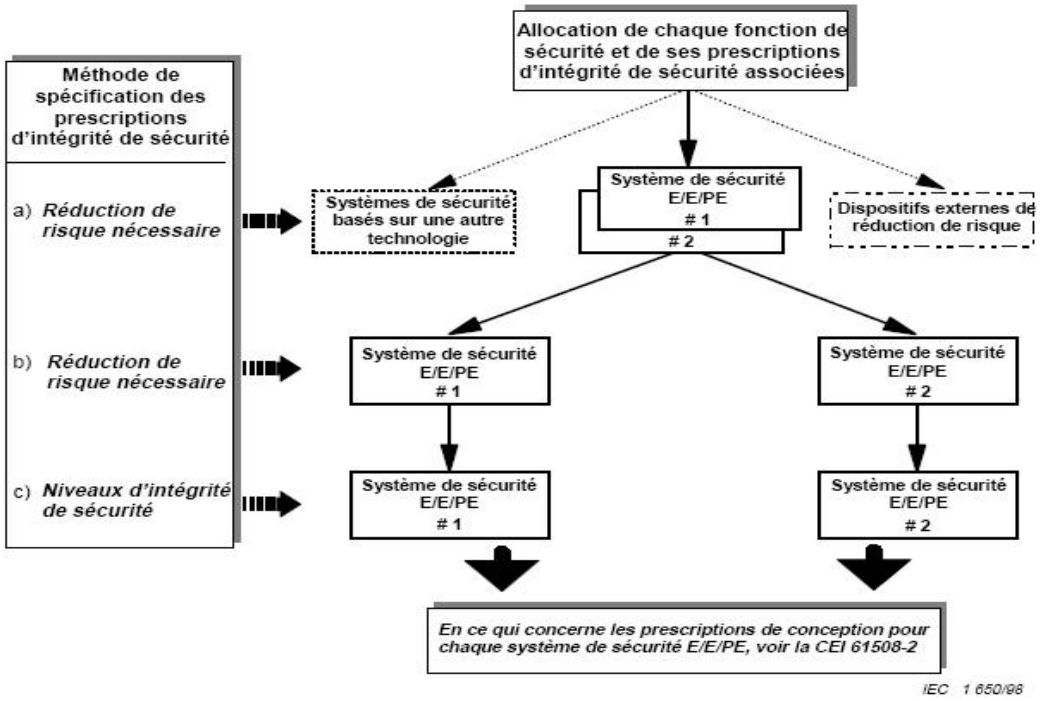

Figure 1.8 : Allocation des prescriptions de sécurité aux systèmes de sécurité E/E/PE (SIS), systèmes de sécurité basés sur une autre technologie et dispositifs externes de réduction de risque

1.4.2. Systèmes instrumentés de sécurité (*SIS*)

Les systèmes instrumentés de sécurité contribuent, avec les autres niveaux de protection, à la réduction du risque afin d'atteindre le niveau de risque tolérable. Ils constituent, probablement, l'une des mesures de réduction de risque les plus importantes. Sont exposés ci-après la définition et les modes de fonctionnement de ces systèmes.

1.4.2.1. Définition d'un SIS

Un *SIS*, aussi appelé boucle de sécurité, est un ensemble d'éléments (matériel et logiciel) assurant la mise en état de sécurité des procèdes lorsque des conditions prédéterminées sont atteintes.

Pour la norme CEI 61508 [IEC 61508-4, 2002] définit les *SIS* comme suit : « un système E/E/PE (électrique/électronique/électronique programmable) relatifs aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité ».

La norme CEI 61511 [CEI 61511, 2003] définit, quant à elle, les systèmes instrumentés de sécurité comme « système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité. Un *SIS* se compose de n'importe quelle combinaison de capteur(s), d'unité loriquet(s) et d'élément(s) terminal (aux) ».

L'architecture type d'un *SIS* est donnée à la figure 1.9. Voici un descriptif succinct de chacune de ses parties :

- *Sous-système « Eléments d'entrée (S :Sensors) » :* constitué d'un ensemble d'éléments d'entrée (capteurs, détecteurs) qui surveillent l'évolution des paramètres représentatifs du comportement de l'*EUC* (température, pression, débit, niveau…).
- *Sous-système « Unité logique (LS : Logic Solver) » :* comprend un ensemble d'éléments logiques (PLC, API) qui récoltent l'information en provenance du sous-système *S* et réalisent le processus de prise de décision qui s'achève éventuellement, si l'un des paramètres dévie au-delà d'une valeur-seuil, par l'activation du sous-système *FE*.
- *Sous-système « Eléments Finaux (FE) » :* agit directement (vanne d'arrêt d'urgence) ou indirectement (vanne solénoïdes, alarme) sur le procédé pour neutraliser sa dérive en le mettant, en général, dans un état sûr.

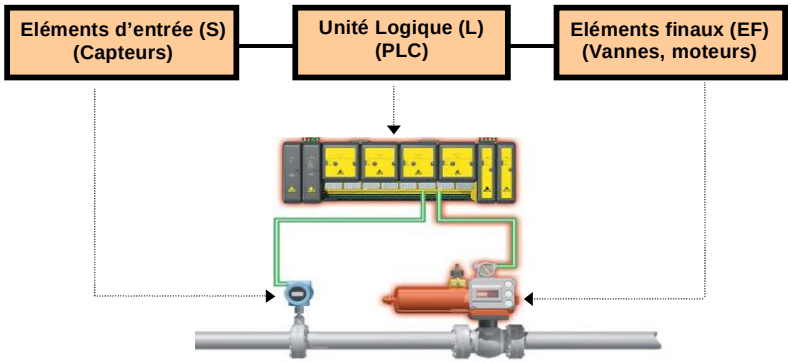

Figure 1.9 : Système instrumenté de sécurité (SIS ou SRS E/E/PE)

Les systèmes suivants en sont des exemples :

- Système d'arrêt d'urgence (*ESD : Emergency Shutdown Systems*), utilisé, par exemple, dans les industries chimique et pétrochimique.
- Système d'arrêt automatique de train (*ATS : Automatic Train Stop*), utilisé dans le domaine ferroviaire.
- Système de freinage de l'automobile.
- Air-bag.
- Système de détection de surface d'un avion.
- Equipements médicaux critiques de traitement et de surveillance.

1.4.2.2. Intégrité de sécurité

La référence [CEI 61508-4, 2002] la définit comme suit : *«probabilité pour qu'un système relatif à la sécurité (SRS) exécute de manière satisfaisante les fonctions de sécurité requises dans toutes les conditions spécifiées et pour une période de temps spécifiée»*. Elle indique également que cette définition est centrée sur la fiabilité des *SRS* dans l'exécution de leurs fonctions de sécurité.

Cette même référence, précise que l'intégrité de sécurité comprend l'intégrité de sécurité du matériel ainsi que l'intégrité de sécurité systématique. Elles sont définies ci-après.

- *Intégrité de sécurité du matériel :* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité liée aux défaillances aléatoires du matériel en mode de défaillance dangereux.
- *Intégrité de sécurité systématique :* partie de l'intégrité de sécurité des systèmes relatifs à la sécurité qui se rapporte aux défaillances systématiques dans un mode de défaillance dangereux, en précisant que l'intégrité systématique ne peut normalement, ou précisément, être quantifiée, mais simplement considérée d'un point de vu qualitatif.

Les deux types de défaillances, aléatoires du matériel et systématiques, définis par la norme CEI 61508 seront explicités dans le prochaine chapitre.

Les prescriptions concernant l'intégrité de sécurité des fonctions de sécurité à allouer aux *SIS* sont spécifiées en termes de niveau d'intégrité de sécurité (*SIL*) : niveau discret parmi quatre possibles, le *SIL* 4 possède le plus haut degré d'intégrité de sécurité. Sa détermination dépend du mode de fonctionnement du *SIS*. Ce point est évoqué dans ce qui suit.

1.4.2.3. Modes de fonctionnement d'un SIS et mesures cibles de défaillances

Une fois le risque tolérable défini et la réduction nécessaire du risque estimée, les exigences d'intégrité de sécurité affectées au *SIS*, pour chaque fonction de sécurité, doivent être spécifiées (en termes de *SIL*) en fonction des mesures cibles de défaillances (voir tableau 1.1).

La notion de mesure cible de défaillances est désignée en matière de probabilité de défaillance dangereuse. Sa vocation diffère selon le mode de fonctionnement du système instrumenté de sécurité [CEI 61508-1, 2000] :

- *Probabilité moyenne de défaillance* lors de l'exécution sur demande de la fonction spécifiée (PFD_{moy}), en mode demande faible. Ce mode de fonctionnement correspond à une fréquence de sollicitation du *SIS* inférieure ou égale à 1 an^{-1} et également inférieure ou égale au double de la fréquence des tests périodiques auxquels il est soumis [CEI 61508-4, 2002].
- *Probabilité d'une défaillance dangereuse par heure* (*PFH*), en mode demande élevée ou en mode continu. Ce second mode correspond à une fréquence de sollicitation du *SIS* supérieure à 1 an^{-1} ou supérieure au double de la fréquence des tests périodiques mentionnés précédemment [CEI 61508-4, 2002].

Une analyse détaillée concernant les modes de fonctionnement d'un *SIS* est donnée dans la référence [INNAL, 2008].

Les valeurs numériques des mesures cibles de défaillances, en fonction du mode d'opération du *SIS*, correspondantes aux niveaux d'intégrité de sécurité sont présentées au tableau 1.1.

Niveau d'intégrité de sécurité (SIL)	Mode de fonctionnement à faible sollicitation (PFD_{moy})	Mode de fonctionnement continu ou à forte sollicitation (PFH)
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$

Tableau 1.1 : Niveaux d'intégrité de sécurité (SIL) en fonction des mesures cibles de défaillances

1.4.3. Allocation du niveau d'intégrité de sécurité (*SIL* requis)

Cette allocation est conduite selon certaines méthodes permettant de définir le niveau d'intégrité de sécurité (*SIL*) requis pour une fonction de sécurité. C'est le *SIL* qui doit être atteint par un *SIS* afin de réaliser la réduction nécessaire du niveau de risque. La section suivante donne un aperçu des méthodes, telles que présentées dans les normes CEI 61508 et CEI 61511, de détermination du niveau d'intégrité de sécurité (*SIL*) correspondant à un phénomène dangereux spécifié (scénario d'accident) lors de la phase d'analyse des risques. Elles sont plus ou moins adaptées en fonction du niveau de détail des analyses de risques réalisées (type et détail des informations disponibles). La CEI 61508, dans sa partie 5, et la CEI 61511 décrivent deux types de méthodes : qualitatives et quantitatives.

1.4.3.1. Méthodes qualitatives

La norme CEI 61508 reconnaît qu'une approche quantitative pour déterminer le niveau d'intégrité de sécurité (SIL) d'une fonction instrumentée de sécurité (*SIF*) n'est pas toujours possible et qu'une approche alternative pourrait parfois être appropriée. Cette alternative consiste en un jugement *qualitatif*. Quand une méthode qualitative est adoptée, un certain nombre de paramètres de simplification doivent être introduits. Ils permettent de qualifier le phénomène dangereux (accident) en fonction des connaissances disponibles. Les normes CEI 61508 et 61511 présentent deux méthodes qualitatives.

- ***Le graphe de risque***

Cette méthode a été introduite par la norme allemande DIN V 19250 [DIN V 19250, 1994], afin de pouvoir exprimer le risque sous forme de classes. La démarche est fondée sur l'équation caractérisant le risque (R) sans considérer les moyens instrumentés de sécurité : $R = f \cdot C$, où f et C sont respectivement la fréquence et la conséquence de l'événement dangereux en l'absence de *SIS*.

La fréquence de l'événement dangereux f est généralement composée de trois facteurs :

F : la fréquence et la durée d'exposition aux dangers,
P : la possibilité d'éviter l'événement dangereux,
W : la probabilité de l'occurrence de l'événement dangereux sans moyen de protection (probabilité de l'occurrence non souhaitée).

La combinaison des quatre paramètres précédents (C, F, P, W) peut ramener à une configuration comparable à celle présentée à la figure 1.10 [CEI 61508-5, 1998].

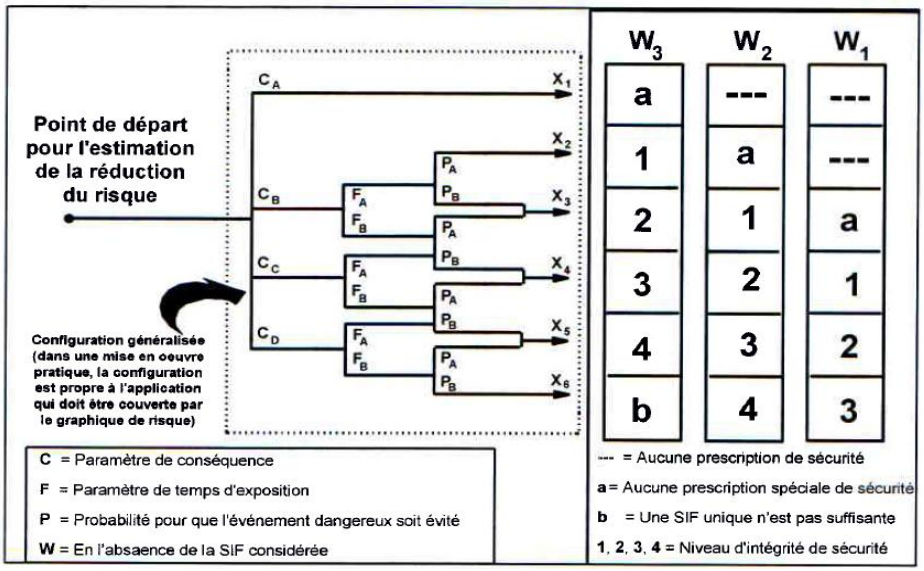

Figure 1.10 : Schéma général du graphe de risque

Le diagramme de risque associe des combinaisons particulières des paramètres de risque aux niveaux d'intégrité de sécurité requis pour la fonction de sécurité instrumentée en prenant en compte le risque tolérable associé au phénomènes dangereux. Les paramètres (*C, F, P, W*) et leur pondération doivent être précisément définis pour chaque situation dangereuse. Une phase de calibrage ou d'étalonnage du graphe de risque est nécessaire. Elle permet d'adapter les paramètres en prenant en compte les spécificités de l'entreprise, la réglementation et les normes du secteur d'application.

- ***Matrice de gravite (matrice de risque, matrice des couches de protection)***

Cette méthode est similaire à la précédente. Elle est utilisée lorsque la fréquence du risque ne peut être quantifiée d'une manière précise. L'analyse débute toujours par l'identification des dangers et leur estimation (fréquence et gravité). Après avoir identifié les différentes couches de protection (chaque couche de protection doit réaliser une réduction d'un ordre de grandeur de SIL (un facteur de 10)), la nécessité d'une couche de protection *SIS* supplémentaire peut être établie en comparent le risque résiduel au niveau de sécurité cible. Ainsi le niveau d'intégrité de sécurité du *SIS* peut être déterminé. Cette méthode suppose l'indépendance des couches de protection. Ces considérations conduisent à la matrice de gravité tridimensionnelle illustrée à la figure 1.11 [CEI 61508-5, 1998].

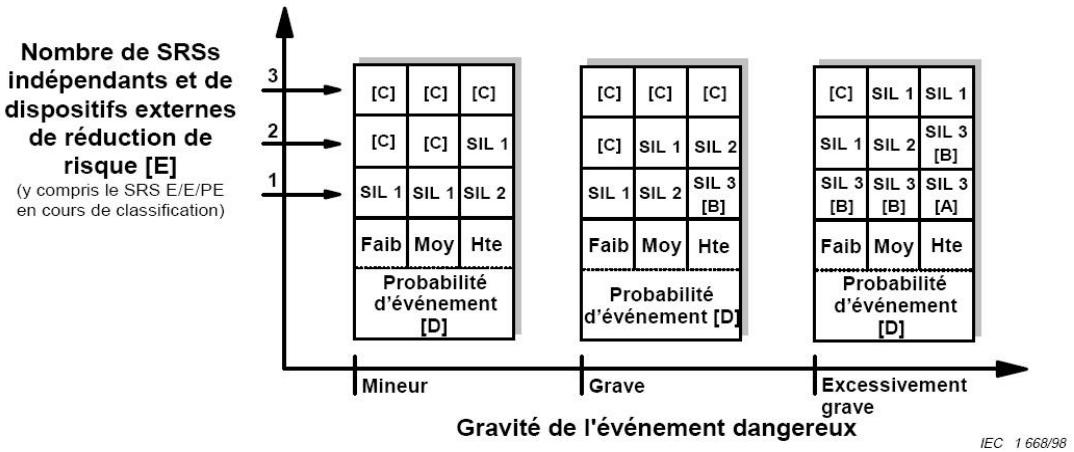

Figure 1.11 : Exemple de matrice de gravité (principes généraux)

Avec :

- **[A]** Un *SRS E/E/PE SIL3* n'apporte pas une réduction suffisante de risque à ce niveau de risque. Des mesures supplémentaires de réduction de risque sont nécessaires.
- **[B]** Un *SRS E/E/PE SIL3* peut ne pas apporter une réduction suffisante de risque à ce niveau de risque. L'analyse des risques et des dangers est requise pour déterminer si des mesures supplémentaires de réduction de risque sont Nécessaires.
- **[C]** Un *SRS E/E/PE* n'est probablement pas nécessaire.
- **[D]** La probabilité d'événement est la probabilité que l'événement dangereux survienne sans système relatif à la sécurité ou sans dispositif externe de réduction de risque.
- **[E]** La probabilité d'événement et le nombre total de couches de protection indépendantes sont définis en relation avec l'application spécifique.

1.4.3.2. Méthodes quantitatives

Ces méthodes sont les plus rigoureuses et les plus précises. L'estimation quantitative de la fréquence de l'événement dangereux (redouté) en constitue la base. La mise en œuvre d'une méthode quantitative nécessite les éléments suivants :

- La mesure cible de sécurité (fréquence tolérable d'accident : $\boldsymbol{F_t}$) doit être spécifiée de façon numérique (par exemple, une conséquence donnée ne devrait pas se produire avec une fréquence supérieure à 1/10000 ans).
- La réduction du risque peut être définie numériquement. Ceci suppose la disponibilité des données numériques suivantes :
  - La fréquence de l'événement initiateur : $\boldsymbol{F_{EI}}$. Elle peut être obtenue en utilisant le retour d'expérience, le jugement d'expert ou encore en utilisant des méthodes de prédiction appropriées (AdD, Chaînes de Markov, etc).
  - Les probabilités de défaillances des couches de protection : ***PFD***.

La méthode quantitative la plus utilisée pour l'allocation des niveaux d'intégrité de sécurité est celle fondée sur principe d'analyse par couches de protection (*LOPA* : *Layers Of Protection Analysis*), voir figure 1.12 [CEI 61511, 2003] [CCPS, 2001]. Elle a été développée à la fin des années 1990 par le CCPS (*Centre for Chemical Process Safety*) [CCPS, 2001]. Cette méthode intègre toutes les couches de protection de l'installation, tant organisationnelles que techniques. Elle évalue la réduction du risque en analysant la contribution des différentes couches [LANTERNIER ET ADJADJ, 2008]. Son principe, rappelons-le, est d'estimer le risque résiduel, exprimé en fréquence d'accident, en quantifiant la fréquence de l'événement initiateur et les probabilités (moyennes) de défaillance sur demande de chaque couche.

Ces couches peuvent être de prévention (diminution de la fréquence de l'occurrence de l'évènement dangereux) ou de protection (réduire les impactes de l'événement dangereux). Une condition majeure qui doit être satisfaite est l'indépendance des différentes couches de protection (*IPL : Independant Protection Layers*). Le tableau 1.2 illustre un exemple de format de la feuille de calcul que l'on peut utiliser lors d'une étude *LOPA*.

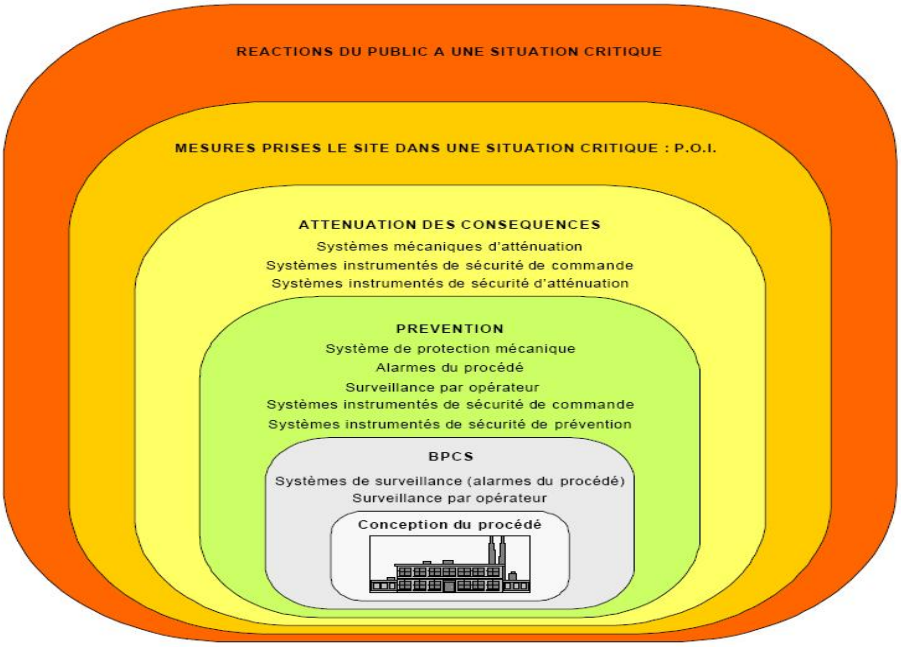

Figure 1.12 : Concept d'analyse par couches de protection (LOPA)

N°	1	2	3	4		5		6	7	8	9	10	11
					COUCHES DE PROTECTION								
	Description de l'événement à impact F.3 F.14.1	Degré de gravité F.4 F.14.1	Cause initiatrice F.5 F.14.2	Probabilité d'occurrence d'une cause initiatrice F.6 F.14.3	Conception générale du procédé F.14.4	BPCS F.14.5	Alarmes, etc. F.14.6	Atténuation supplémentaire, accès limité,F.8 F.14.7	IPL Digues d'atténuation supplémentaire, détente F.9 F.14.8	Probabilité intermédiaire d'occurrence d'événement F.10 F.14.9	Niveau d'intégrité d'une SIF F.11 F.14.10	Probabilité d'événement atténué F.12 F.14.10	Notes
1	Incendie dû à une rupture de la colonne de distillation	S	Perte d'eau de refroidissement	0,1	0,1	0,1	0,1	0,1	PRV 01	10^{-7}	10^{-2}	10^{-9}	Une pression élevée a provoqué une rupture de colonne
2	Incendie dû à une rupture de la colonne de distillation	S	Défaillance de la boucle de régulation de la vapeur	0,1	0,1		0,1	01	PRV 01	10^{-8}	10^{-2}	10^{-9}	Idem ci-dessus
N													

NOTE Degré de gravité E = Très grave; S = Grave; M = Mineur.
Les valeurs des probabilités d'occurrence sont des événements par année, d'autres valeurs numériques sont des probabilités de défaillance sur sollicitation moyenne.

Tableau 1.2 : Exemple de tableau LOPA

La fréquence de l'événement redouté (scénario d'accident : colonne n°10 du tableau 1.2) s'obtient en multipliant la fréquence de l'événement initiateur et les probabilités moyennes de défaillance à la demande (PFD_{moy}) de chaque *IPL* s'opposant à cet même événement.

$$f^{C} = f^{IE} \times \prod_{i} PFD_{moy}^{i} \qquad (1.1)$$

où :

f^{C} : fréquence de réalisation de la conséquence *C*,
f^{IE} : fréquence de l'événement initiateur,

PFD_{moy}^{i} : Probabilité moyenne de défaillance sur demande de la barrière *i*. L'équipe *LOPA* doit déterminer cette quantité pour chaque barrière considérée.

La réduction du risque assignée à la fonction de sécurité du *SIS* s'obtient en comparant la fréquence de l'événement redouté à l'objectif de sécurité (fréquence tolérable : f_t).

$$PFD_{moy}^{SIS} \leq \frac{f_t}{f^{IE} \times \prod_{i \neq SIS} PFD_{moy}^{i}} \tag{1.2}$$

La quantité correspondante au membre droit de l'inégalité (1.2) représente la probabilité moyenne de défaillance maximale que le *SIS* pourrait avoir, tel que la réduction de risque nécessaire soit réalisée. La lecture de cette quantité dans le tableau 1.1 permet de définir le *SIL* correspondant.

L'inégalité (1.2) telle que écrite n'est valable que pour le mode de fonctionnement faible demande. Pour le mode de fonctionnement demande élevée ou continu, il serait nécessaire de dimensionner la fréquence de l'événement initiateur qui représente, dans ce cas de figure, la *PFH* du *SIS* :

$$PFH_{SIS} \leq \frac{f_t}{\prod_{i \neq SIS} PFD_{moy}^{i}} \tag{1.3}$$

Il est important de noter que dans le cas où des relations de dépendance existent entre les différentes barrières, il serait plus convenable d'utiliser des approches de modélisation plus appropriées (arbre des défaillances, chaînes de Markov, Réseaux de Petri, …).

1.4.4. Adéquation des *SIS* aux niveaux d'intégrité de sécurité requis (*SIL* réel)

La norme CEI 61508 montre que la satisfaction aux mesures cibles de sécurité (SIL requis) se fait par l'observation simultanée des trois prescriptions suivantes :

- ***Prescriptions qualitatives*** : minimisation de l'occurrence des défaillances systématiques par l'application des différentes prescriptions pendant les différentes phases du cycle de vie de sécurités du *SIS*.

  Ce volet n'est pas couvert par mes travaux de recherche.

- ***Prescriptions quantitatives (probabilistes)*** : par le calcul de la probabilité moyenne de défaillance (PFD_{moy}), ou par heure (*PFH*), du *SIS* due exclusivement à des défaillances aléatoires du matériel. Si la mesure cible du risque (en d'autre terme, le *SIL* spécifié lors de l'analyse des risques) n'est pas remplie, la conception du *SIS* sera changée jusque à la satisfaction de la mesure cible.

  Les différentes formulations analytiques permettant le calcul des PFD_{moy} et *PFH* constituent l'objet du second chapitre de ce document.

- ***Contraintes architecturales.*** La détermination du *SIL* de manière probabiliste via le calcul de la valeur moyenne de la *PFD* ou de la *PFH*, n'offrirait pas la garantie d'une précision suffisante, selon la norme CEI 61508. Il conviendrait donc de confirmer ou de corriger la valeur ainsi trouvée pour le *SIL* en appliquant une autre méthode de détermination, de nature différente : la prise en compte des les contraintes architecturales.

Les *contraintes* architecturales représentent, d'une certaine manière, une première estimation de la capacité d'un système instrumenté à accomplir sa fonction en analysant son architecture. Les contraintes d'architectures ont généralement pour effet de limiter le niveau d'intégrité de sécurité pouvant être atteint.

Il est écrit dans la norme 61508-2 que, « *dans le contexte de l'intégrité de sécurité du matériel le niveau d'intégrité le plus élevé qui peut être annoncé pour la fonction de sécurité donnée est limité par la tolérance aux anomalies du matériel et la proportion de défaillances en sécurité des sous-systèmes qui réalisent la fonction de sécurité* ».

La norme définit alors ces deux nouveaux termes :

- Une *tolérance aux anomalies du matériel* N signifie que (N+1) anomalies sont susceptibles de provoquer la perte de la fonction de sécurité.
- La *proportion de défaillances en sécurité* d'un sous-système (*SFF : Safe Failure Fraction*) est définie par le rapport du taux moyen des défaillances en sécurité, plus les défaillances dangereuses détectées au taux de défaillance moyen total du sous-système.

La démarche présentée dans l'annexe C de la norme 61508-2 s'appuie sur deux tableaux reproduits ci-après.

Proportion de défaillances en sécurité (SFF)	***Tolérance aux anomalies matérielles***		
	0	**1**	**2**
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4
Un SIS peut être considéré du type A si son comportement en présence d'anomalies est bien déterminé, si les modes de défaillance de ses constituants sont bien définis et si les données concernant leurs défaillances, issus du retour d'expérience, sont connus avec une bonne fiabilité.			

Tableau 1.3 : Contraintes architecturales sur les SIS du type A

Proportion de défaillances en sécurité (SFF)	***Tolérance aux anomalies matérielles***		
	0	**1**	**2**
< 60 %	Non autorisé	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
>= 99 %	SIL 3	SIL 4	SIL 4
Un SIS peut être considéré du type B si une des trois conditions régissant le type A n'est pas satisfaite.			

Tableau 1.4 : Contraintes architecturales sur les SIS du type B

Pour chaque sous-système d'un *SIS* qui participent à la réalisation d'une fonction de sécurité, on calcule la *SFF* et la tolérance aux anomalies (N = 0 à 2). Le croisement de ces deux entrées orthogonales donne, pour chacun des tableaux précédents, la valeur maximale du *SIL* qu'on peut annoncer pour chaque sous-système.

Il convient de mentionner que les tableaux relatifs aux contraintes d'architecture présentés dans la CEI 61511 diffèrent des tableaux 1.3 et 1.4.

1.5. Conclusion

Au cours du premier chapitre, nous avons d'abord rappelé certaines définitions des termes fondamentaux ayant trait au domaine de la gestion des risques. A ce titre, la démarche générale de la gestion des risques a également été présentée et brièvement expliquée. Puis nous avons précisé l'organisation de la norme CEI 61508 et défini les systèmes instrumenté de sécurité, qui sont utilisés pour détecter des situations dangereuses et diminuer leurs conséquences pour atteindre des niveaux de risques tolérables. Il convient à cet effet de rappeler que la CEI 61508 de même que ses normes filles sont actuellement devenues la référence par excellence pour la mise en œuvre des ce type de systèmes. Nous avons précisé que la démarche générale de la CEI 61508 s'appuie sur le principe du cycle de vie de sécurité, dont l'analyse des risques en constitue le pilier capital. Cette étape permet de définir la réduction nécessaire du risque que le *SIS* doit assurer, en matière de niveaux d'intégrité de sécurité (*SIL*).

Les principales méthodes d'allocation des niveaux d'intégrité de sécurité requis aux fonctions de sécurité implémentées par des *SIS* ont ensuite été décrites. Nous avons vu que ces méthodes peuvent être aussi bien qualitatives que quantitatives. Le choix de la méthode de travail dépend principalement de la nature des données dont le groupe d'analyse dispose. En effet, les techniques qualitatives dépendent largement du degré d'expertise du groupe de travail. Un jugement qualitatif est souvent difficile à obtenir, surtout lorsque l'installation est trop complexe ou lorsque le retour d'expérience est pauvre (cas des nouvelles technologies). Il n'est pas étonnant que le SIL obtenu puisse facilement varier selon la manière d'appréciation des paramètres qui caractérise le risque. Néanmoins, l'approche qualitative peut être employée avec de bons résultats selon le niveau d'expertise et la complexité des systèmes. Sa mise en œuvre est simple et nécessite peu de moyens et de temps. De plus, elles constituent une excellente base pour identifier certains points, relatifs au système étudié, qui peuvent faire l'objet d'une analyse plus détaillée. En revanche, les méthodes quantitatives sont plus précises, mais à condition que la qualité des données soit correcte. En plus, et d'une manière générale, les approches quantitatives sont très gourmandes en matières de temps et de ressources.

Finalement, nous avons évoqué les prescriptions que les *SIS* doivent satisfaire afin de réaliser la réduction nécessaire des risques. Elles sont au nombre de trois, rappelons-les :

- *Prescriptions qualitatives* permettant de maîtriser les défaillances systématiques (voir le chapitre suivant pour plus de précisions).
- *Prescriptions probabilistes* : calcul de la PFD_{moy} (fonctionnement en faible demande) ou de la *PFH* (fonctionnement en demande forte ou continue). Ces deux grandeurs ne doivent pas dépasser les mesures cibles définies au cours de l'étape d'allocation des niveaux d'intégrité de sécurité.
- *Contraintes architecturales* qui ont généralement pour effet de limiter le niveau d'intégrité de sécurité pouvant être atteint en se basant sur la seule considération des PFD_{moy} et *PFH*. Les contraintes d'architecture remédient, selon la CEI 61508, en quelque sorte aux incertitudes qui entachent les données fiabilistes relatives aux constituants des *SIS*.

Le prochain chapitre est consacré à la présentation et l'étude des différentes formulations mathématiques relatives aux performances probabilistes des *SIS*, à savoir : PFD_{moy}, *PFH*, PFS_{moy} et *STR*.

CHAPITRE 2

Probabilités de défaillances dangereuse et sûre (*PFD – PFH / PFS – STR*)

2.1. Introduction

Comme indiqué au niveau du premier chapitre, une évaluation quantitative des performances probabilistes (mesures cibles de défaillance) des systèmes instrumentés de sécurité constitue une étape indispensable pour la validation de ces systèmes. Cette validation n'est autre que l'assurance que ces derniers peuvent effectivement réaliser la réduction nécessaire du risque (***intégrité de sécurité*** requise).

En plus des prescriptions affichées dans la norme, qui ont pour but de satisfaire aux objectifs de sécurité, il est nécessaire de prendre en compte toute perturbation, imputable aux *SIS*, sur le fonctionnement nominal du système surveillé (*EUC*) en absence de situations dangereuses. Ces perturbations sont généralement dues aux déclenchements intempestifs des *SIS*, qui provoquent l'arrêt de l'outil de production.

Pour les industriels, il est donc incontestable de réduire aux maximum possible ce type de déclenchements. A cet effet, l'évaluation quantitative des performances des *SIS* au regard des déclenchements intempestifs n'en présente pas moins d'importance que celle préconisée dans la CEI 61508. On parle, à ce titre, d'***intégrité opérationnelle*** des *SIS*.

La satisfaction aux objectifs d'intégrité de sécurité et d'intégrité opérationnelle passe par un choix adéquat de l'architecture du *SIS* à mettre en place. Ce choix constitue nécessairement un compromis optimal entre ces deux objectifs.

Afin d'optimiser l'architecture d'un *SIS*, il est nécessaire, dans un premier temps, de définir sans ambiguïté l'ensemble des grandeurs y contribuant. Parmi ces grandeurs, les indicateurs d'intégrité de sécurité (*PFD/PFH*) et les indicateurs d'intégrité opérationnelle (*PFS/STR*) ont été retenus dans le cadre de ce travail.

Dans la suite de ce chapitre nous exposons, dans un premier temps, la typologie des défaillances liée aux systèmes instrumentés de sécurité. Ceci permet de bien apprécier les indicateurs probabilistes cités précédemment. Nous présentons ensuite les différentes formulations analytiques, retrouvées dans la littérature, de ces indicateurs, et ce, pour les architectures systèmes *KooN* les plus utilisées. Est également donné un échantillon de résultats à des fins de comparaison.

2.2. Classification des défaillances

Pour une meilleure compréhension des formules analytiques liées aux différentes grandeurs probabilistes évoquées dans ce manuscrit, une clarification des différentes paramètres fiabilistes, caractérisant les éléments constitutifs des *SIS*, s'impose. Cette clarification concerne en premier lieu la classification des défaillances qui entraînent l'inhibition ou l'activation (intempestive) de la fonction de sécurité.

2.2.1. Classification des défaillances selon leurs causes

L'étude des défaillances des systèmes montre l'existence de deux catégories de défaillances : les défaillances physiques (aléatoires du matériel) et les défaillances fonctionnelles (systématiques) [GOBLE, 1998].

La norme CEI 61508 adopte la même classification. La définition des défaillances aléatoires du matériel donnée par cette norme est la suivante : *«défaillances survenant de manière aléatoire et résultant de divers mécanismes de dégradations au sein du matériel»*. Une telle défaillance rend donc le système incapable de remplir sa fonction suite à sa dégradation physique. Il est important de noter que la dégradation physique du système à deux causes principales :

- *Vieillissement du matériel.* Les défaillances dues au vieillissement sont appelées *défaillances naturelles ou primaires.*

- *Exposition aux contraintes excessives* : ces contraintes peuvent être induites par des facteurs externes ou par des erreurs humaines. Ces défaillances sont appelées *défaillances secondaires*.

Les défaillances aléatoires du matériel sont relativement bien comprises. Les données relatives à cette catégorie de défaillances sont, dans la plupart du temps, disponibles.

La défaillance systématique est définie par la même norme comme étant *« défaillance reliée de façon déterministe à une certaine cause, ne pouvant être éliminée que par une modification de la conception ou du processus de fabrication, des procédures d'exploitation, de la documentation ou d'autres facteurs appropriés»*. Lors de l'occurrence d'une telle défaillance, le système ne remplie plus la fonction qui lui est demandée, mais il ne présente aucune dégradation physique. C'est la raison pour laquelle ces défaillances sont qualifiées de non physiques ou de fonctionnelles (par exemple : l'opérateur ferme une vanne par erreur, la vanne dans ce cas n'est pas dégradée physiquement).

Les défaillances systématiques peuvent être divisées en deux catégories :

- *Défaillances de conception* : ces défaillances sont introduites lors de l'une des phases du cycle de vie du système. Elles existent à l'état latent, se révèlent lors du fonctionnement du système et ne peuvent généralement être éliminées que par une modification de la conception ou du processus de fabrication. Des exemples typiques de ces défaillances sont les défauts de conception du logiciel et du matériel.
- *Défaillances d'interactions* : ces défaillances sont initiées par les erreurs humaines lors de l'exploitation, la maintenance,…

La norme CEI 61508 considère que les défaillances du logiciel sont toutes systématiques. Par opposition aux défaillances aléatoires du matériel, les défaillances systématiques sont difficiles à modéliser et de ce fait moins compréhensibles. Elles ne sont pas prises en compte dans les formules analytiques proposées par la CEI 61508.

Cette classification de défaillances est résumée à la figure 2.1.

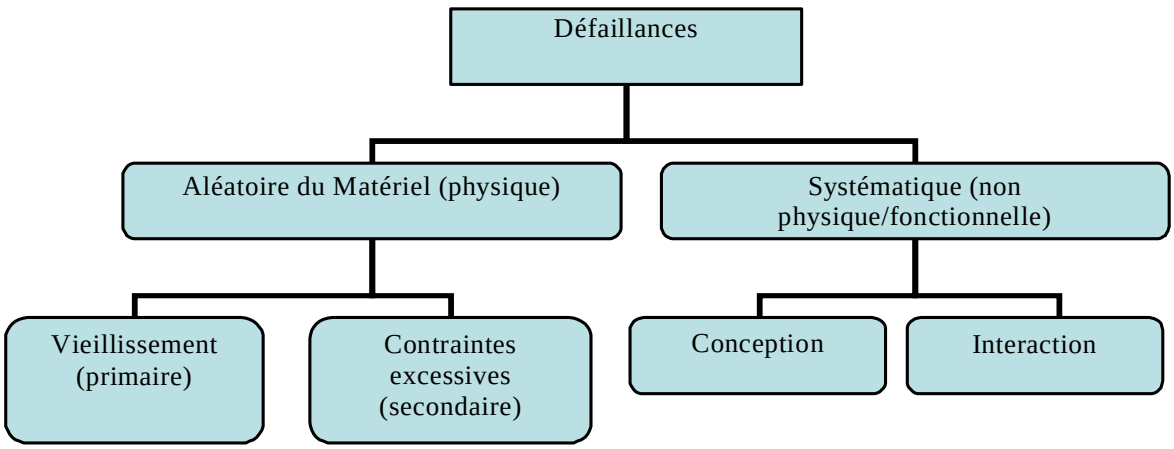

Figure 2.1: Classification des défaillances selon leurs causes

La prise en compte des défaillances systématiques dans l'évaluation de la performance des *SIS* est primordial, une étude du UK HSE (Health Safety & Environnemental Agency) le confirme [HSE, 1995]. Cette étude, qui a concernée 34 accidents, a montré que 85% de l'ensemble des défaillances des *SIS* sont des défaillances systématiques et prés de 60% de ces défaillances sont dues à des opérations avant même l'installation des SIS (voir figure 2.2).

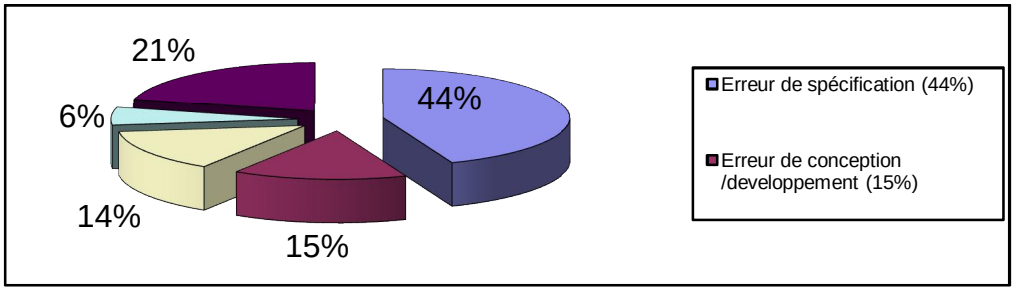

Figure 2.2 : Répartitions des causes des défaillances systématiques

La prise en compte simultanée de ces deux types de défaillances est importante dans l'évaluation des performances des *SIS*. A ce titre, la norme CEI 61508 exige le traitement de l'ensemble des défaillances afin d'assurer l'intégrité de sécurité du *SIS*. La figure 2.3 illustre la manière selon laquelle cette norme traite ces défaillances.

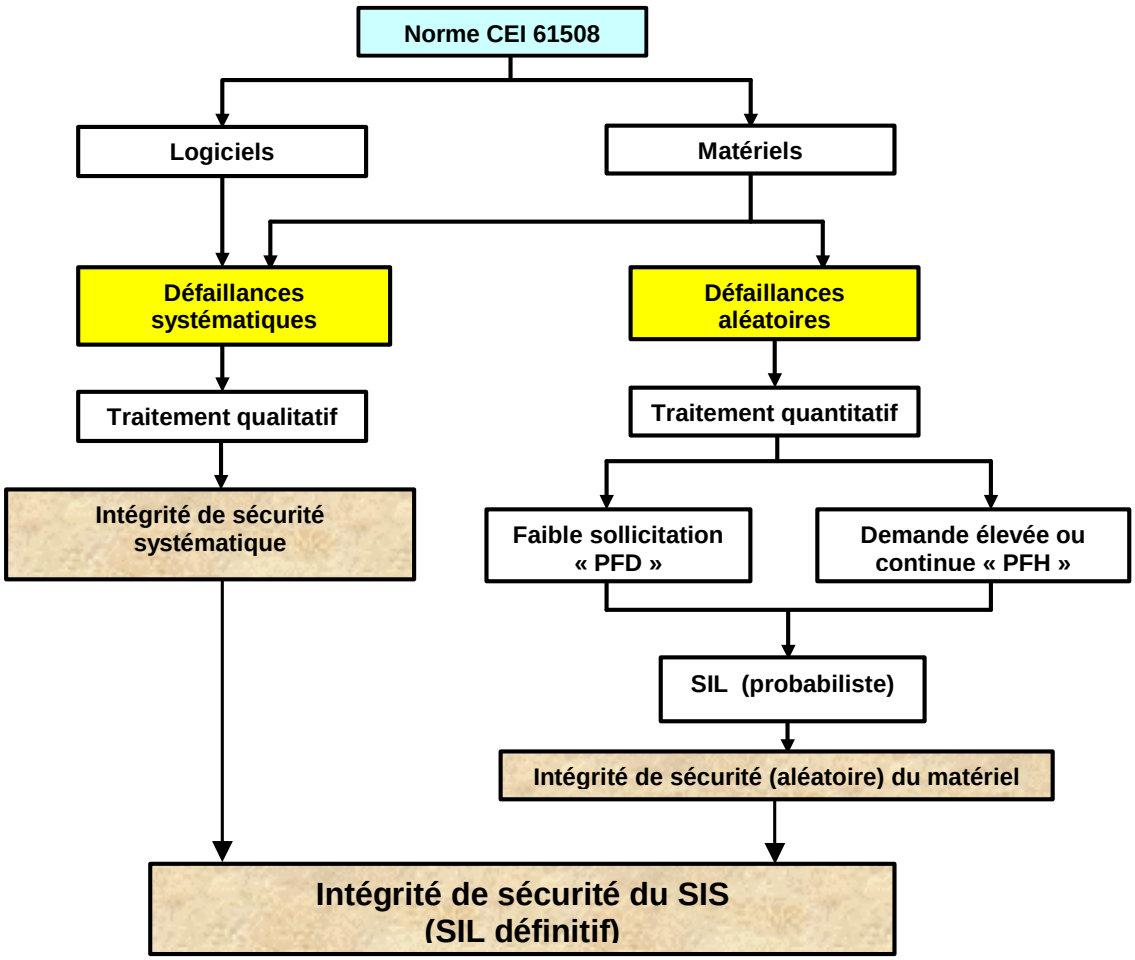

Figure 2.3 : Traitement des défaillances systématiques et aléatoires selon la CEI 61508

2.2.2. Classification des défaillances selon leurs effets sur la fonction de sécurité

Toutes les défaillances (aléatoires du matériel et systématiques), selon leurs effets, peuvent être classées dans l'une des deux catégories suivantes : *défaillances en sécurité* (*safe failures*) ou *défaillances dangereuses* (*dangerous failures*).

Suivant cette dernière classification, seules les défaillances aléatoires du matériel sont prises en compte dans ce qui suit. Dans ces conditions, les définitions de ces deux catégories selon la norme CEI 61508 sont données ci-après :

- *Défaillance dangereuse* : *«défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction »*.
- *Défaillance en sécurité* : *« défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction »*.

En nous situant donc dans le contexte de la CEI 61508, une défaillance dangereuse est une défaillance qui tend à inhiber la fonction de sécurité en cas de demande émanant de l'*EUC* qui sera alors dans un état dangereux. Une défaillance sûre est une défaillance intempestive qui tend à anticiper le déclenchement de la fonction de sécurité, en l'absence de toute demande, en conduisant effectivement l'*EUC* dans un état sûr. C'est-à-dire tel que l'occurrence de tout événement dommageable n'y est plus possible.

Compte tenu de cette décomposition, le taux de défaillance aléatoire du matériel de chaque canal (λ) comporte deux composantes :

$$\lambda = \lambda_S + \lambda_D \qquad (2.1)$$

avec :

λ_S : taux de défaillance aléatoire en sécurité du matériel,

λ_D : taux de défaillance aléatoire dangereuse du matériel.

Une autre partition résulte du fait que ces défaillances peuvent être ou non détectées par des tests en ligne (tests de diagnostic). Les premières sont dénommées défaillances détectées (*detected failures*) et les secondes, qui ne peuvent être révélées que lors des tests périodiques hors ligne ou lors de la sollicitation du *SIS* par le système surveillé, sont dénommées défaillances non détectées (*undetected failures*). Le schéma suivant est classiquement présenté pour résumer cette double partition [IDDIR, 2009].

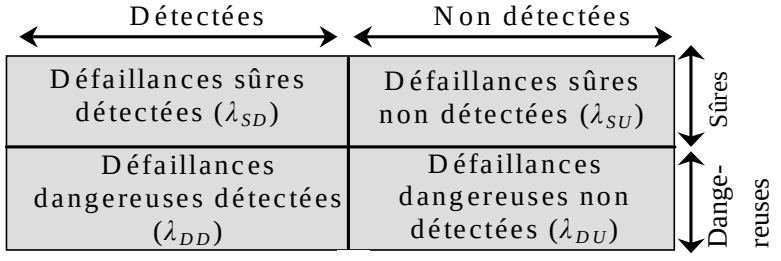

Figure 2.4 : Répartition des défaillances et de leurs taux selon la norme CEI 61508

Il convient de signaler que l'organisme norvégien SINTEF propose dans son manuel [SINTEF, 2006] une classification proche de la précédente (voir figure 2.5).

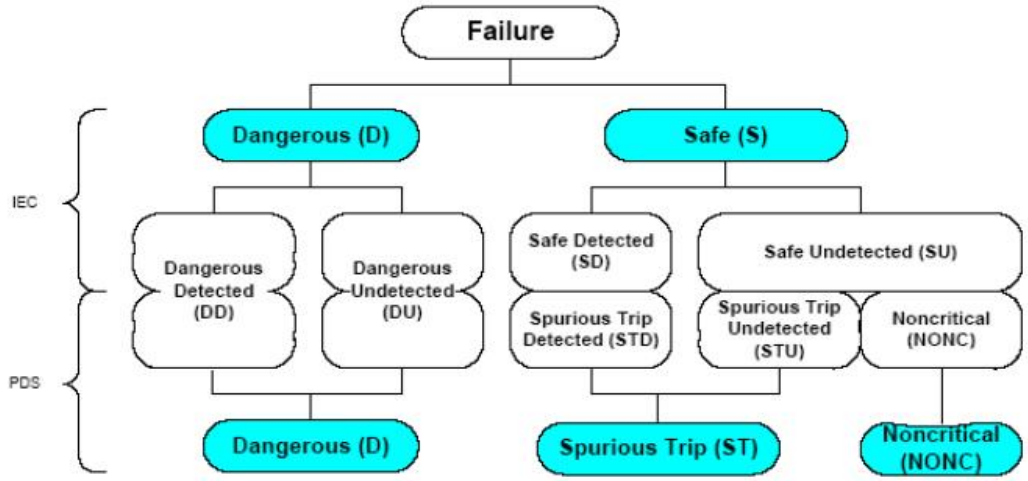

Figure 2.5 : Classification des défaillances selon SINTEF

La lecture de la figure 2.5 nous permet d'écrire les deux équations suivantes :

$$\lambda_D = \lambda_{DD} + \lambda_D \quad (2.2)$$

$$\lambda_S = \lambda_{SD} + \lambda_{SU} \quad (2.3)$$

La capacité d'un *SIS* à détecter ses défaillances « *en ligne* » se résume dans son taux de couverture ou sa couverture de diagnostic *DC* (*Diagnostic Coverage*). Cette couverture est exprimée par un nombre allant de 0 à 1, ou comme un pourcentage.

En introduisant la couverture de diagnostic, on peut récrire les différents taux de défaillances, évoqués précédemment, comme suit :

$$\lambda_{DD} = DC \,.\, \lambda_D \quad (2.4)$$

$$\lambda_{DU} = (1\text{-}DC) \,.\, \lambda_D \quad (2.5)$$

DC représente la couverture de diagnostic des défaillances aléatoires dangereuses.

$$\lambda_{SD} = DC_S \,.\, \lambda_S \quad (2.6)$$

$$\lambda_{SU} = (1\text{-}\, DC_S) \,.\, \lambda_S \quad (2.7)$$

Ici, DC_S représente la couverture de diagnostic des défaillances aléatoires en sécurité.

Par ailleurs, il existe des défaillances qui peuvent affecter simultanément tout les canaux constitutifs d'une architecture redondante : les défaillances de cause commune (*DCC ou CCF pour Common Cause F/ailure*). Pour estimer leur taux de défaillance (λ_{DCC}), la CEI 61508 utilise le *modèle du facteur* β :

$$\lambda_x = \lambda_{x_{ind}} + \lambda_{x_{DCC}} = (1\text{-}\beta_x)\lambda_x + \beta_x \lambda_x \quad (2.8)$$

β_x est le pourcentage des *DCC*. L'indice « *ind* » signifie défaillances indépendantes dont l'occurrence n'affecte qu'un seul composant de l'architecture *KooN*, tandis que « *x* » est utilisé pour rendre compte de la partition précédente des défaillances (*DU, DD, SU, SD*).

Dans ce qui suit nous donnant une description détaillée des différentes architectures *KooN* types : 1*oo*1, 1*oo*2, 1*oo*3, 2*oo*2 et 2*oo*3.

2.3. Architectures *KooN* usuelles

2.3.1. Architecture 1*oo*1

Cette architecture de base est composée d'un seul canal et qu'en conséquence toute défaillance dangereuse induit la perte de la fonction de sécurité en cas de demande. De plus, toute défaillance sûre conduit à l'exécution de cette fonction en absence de demande. Cette architecture minimale, qui ne tolère pas de défaillance, ne peut être utilisée dans des applications de sécurité. Le bloc-diagramme physique ainsi que le schéma électrique de principe relatif à cette architecture sont donnés à la figure 2.6 [CEI 61508-6, 2000] [CHARPENTIER, 2002]. Les diagnostics y sont présents pour assurer la détection des défaillances (dangereuses et sûres) en vue de les réparer immédiatement.

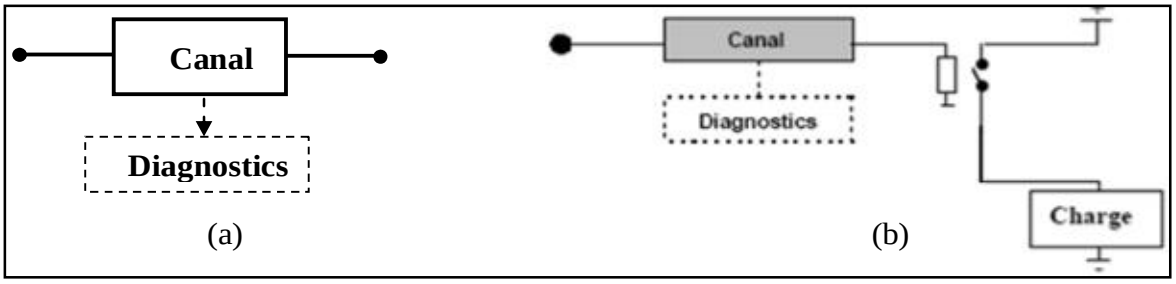

Figure 2.6 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1*oo*1

L'ensemble des schémas électriques présentés dans ce document s'appuient sur le principe « *de-energised to trip* », c'est le *principe du courant au repos*. Les systèmes basés sur ce principe sont conçus de façon à supprimer l'énergie suite à une erreur (une défaillance de l'alimentation, à titre d'exemple). L'exécution de la fonction de sécurité nécessite l'ouverture des relais (coupure de l'alimentation de la charge). Dans ce cas, les défaillances dangereuses se traduisent par le maintien de l'alimentation de la charge (relais fermés), les relais étant initialement fermés, tandis que les défaillances sûres entrainent l'ouverture des relais.

2.3.2. Architecture 1*oo*2

Cette architecture se compose de deux canaux identiques fonctionnant en redondance chaude : chaque canal peut réaliser la fonction de sécurité. Il faut donc que ces deux canaux subissent chacun une défaillance dangereuse pour que le système n'assure pas sa fonction de sécurité en cas de demande. A ce titre, la défaillance sûre de l'un ou l'autre des deux canaux conduit le système surveillé vers un état de repli sûr (activation de la fonction de sécurité).

La figure 2.7 regroupe le bloc-diagramme physique et le schéma électrique relatif à cette seconde architecture.

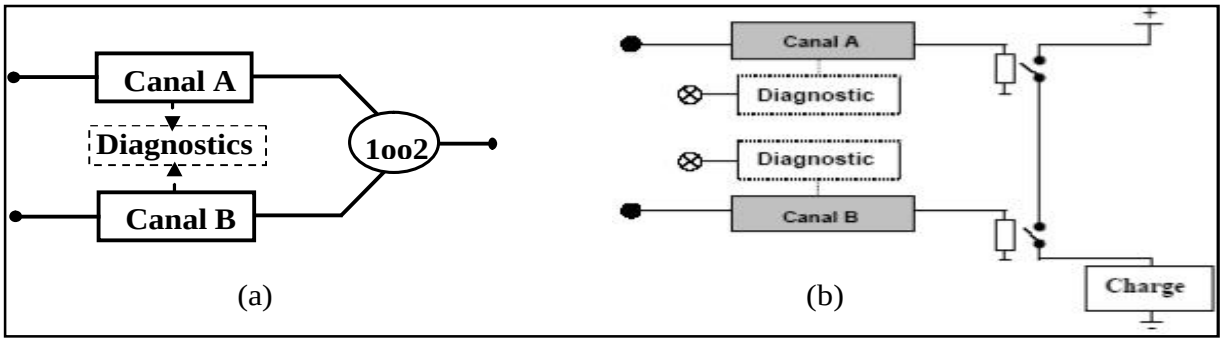

Figure 2.7 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1*oo*2

Le montage « de-energized to trip » se traduit par un schéma série pour lequel une coupure d'énergie provoque un passage en position de sécurité. L'activation de la fonction de sécurité se traduit par l'ouverture des relais de sortie. Si une des voies est défaillante avec sa sortie active (relais fermé), l'autre voie peut désactiver la charge (ouvrir le relais) et assurer la fonction de sécurité [CHARPENTIER, 2002].

Toutes les architectures de type 1*ooN* ont le même principe de fonctionnement. On peut facilement en déduire que le nombre de défaillances dangereuses provoquant l'inhibition de la fonction de sécurité est égale à *N*. En revanche, le nombre de défaillances sûres conduisant au déclenchement intempestif du SIS est égal à 1. C'est aussi le cas de l'architecture suivante : 1*oo*3.

2.3.3. Architecture 1*oo*3

L'architecture 1*oo*3 n'a été traitée que dans la version actuelle de la norme 61508-6 [CEI 61508, 2009]. Cette architecture est composée de trois canaux connectés en parallèle, fonctionnant en redondance active (voir figure 2.8). C'est-à-dire que ce système restera opérationnel, vis-à-vis des défaillances dangereuses, tant qu'au moins un de ces canaux le sera. Cela dit, une seule défaillance sûre provoque l'activation de la fonction de sécurité.

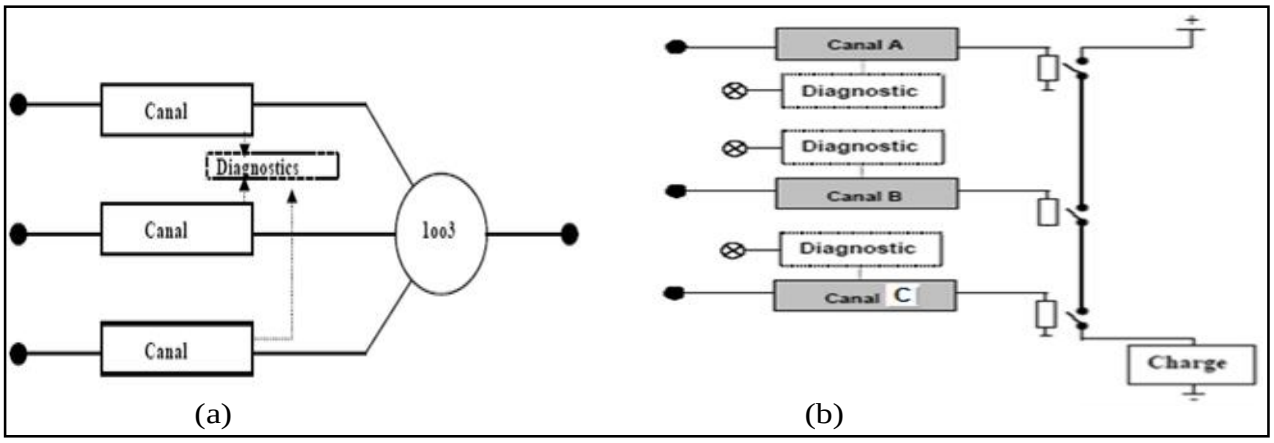

Figure 2.8 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1*oo*3

2.3.4. Architecture 2*oo*2

Cette architecture consiste en deux canaux en parallèle de sorte que les deux canaux doivent demander la fonction de sécurité pour que celle-ci soit activée : fonctionnement série au sens fiabiliste. Le système a donc un comportement dangereux dès qu'une défaillance dangereuse survient dans un des deux canaux. En revanche, le déclenchement intempestif (activation de la fonction de sécurité en absence de demande) ne se réalise que si les deux canaux observent des défaillances sûres.

Le bloc-diagramme physique et le schéma électrique de principe de cette architecture sont donnés à la figure 2.9.

Au niveau du montage « de-energized to trip », la sortie est modélisée par deux relais câblés en parallèle. En fonctionnement normal, l'activation de la fonction de sécurité ouvre les relais correspondants à chaque canal : les deux canaux doivent demander la fonction de sécurité pour que celle-ci soit exécutée. Le système a un comportement dangereux (sortie alimentée alors que la fonction de sécurité est sollicitée), dès qu'une défaillance dangereuse (collage du relais de sortie) survient dans l'un des deux canaux [CHARPENTIER, 2002].

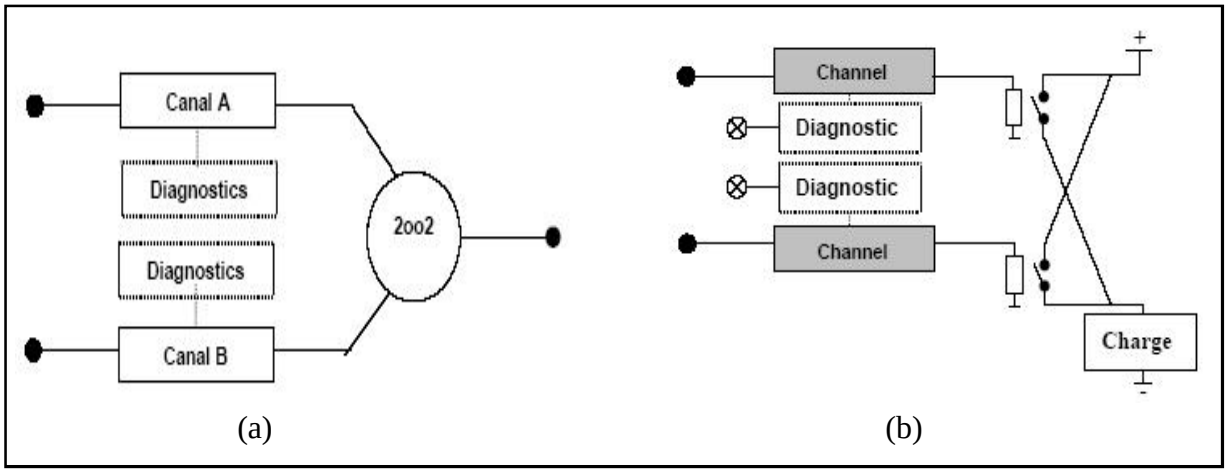

Figure 2.9 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 2*oo*2

Il importe de signaler que pour les architectures séries (*NooN*) une seule défaillance dangereuses engendre la non exécution de la fonction de sécurité en présence de demande, alors que *N* défaillances sûres sont nécessaires pour conduire à un déclenchement intempestif du *SIS*.

2.3.5. Architecture 2*oo*3

Cette architecture comprend trois canaux connectés en parallèle avec un dispositif à logique majoritaire pour les signaux de sortie, de telle sorte que l'état de sortie n'est pas modifié lorsqu'un seul canal donne un résultat différent des deux autres canaux [CEI 61508, 1998], voir figure 2.10. Ceci dit, le nombre de défaillances nécessaires aussi bien à l'empêchement de l'exécution de la fonction de sécurité qu'au déclenchement intempestif du *SIS* s'élève à deux.

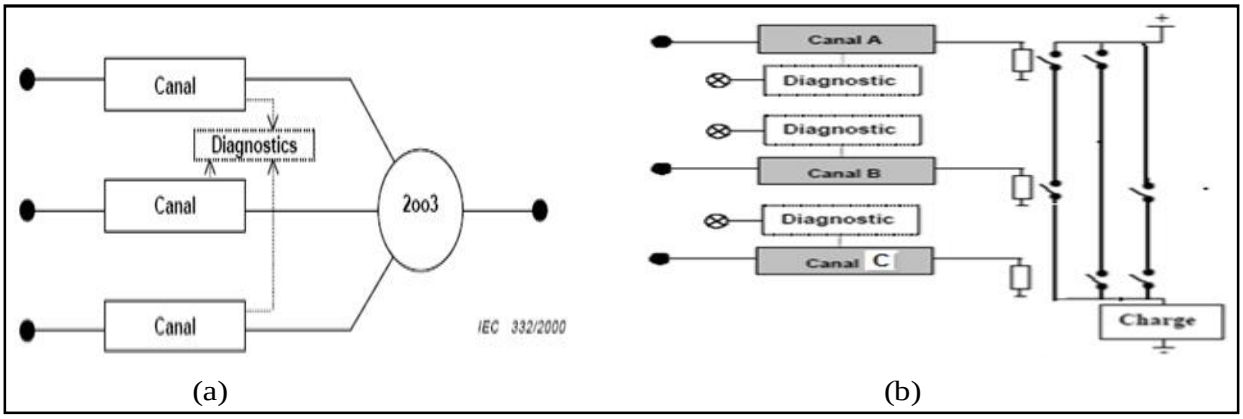

Figure 2.10 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 2*oo*3

D'une manière générale, pour une architecture *KooN* ces deux nombres sont établis ainsi :

- ***N – K*+1** représente le nombre de défaillances dangereuses dont l'occurrence induit la perte de la fonction de sécurité.
- ***K*** représente le nombre de défaillances sûres dont l'occurrence conduit à l'activation intempestive de cette même fonction.

Ce constat est mieux explicité au niveau de la figure 2.11 (DUTUIT et *al.* 2009).

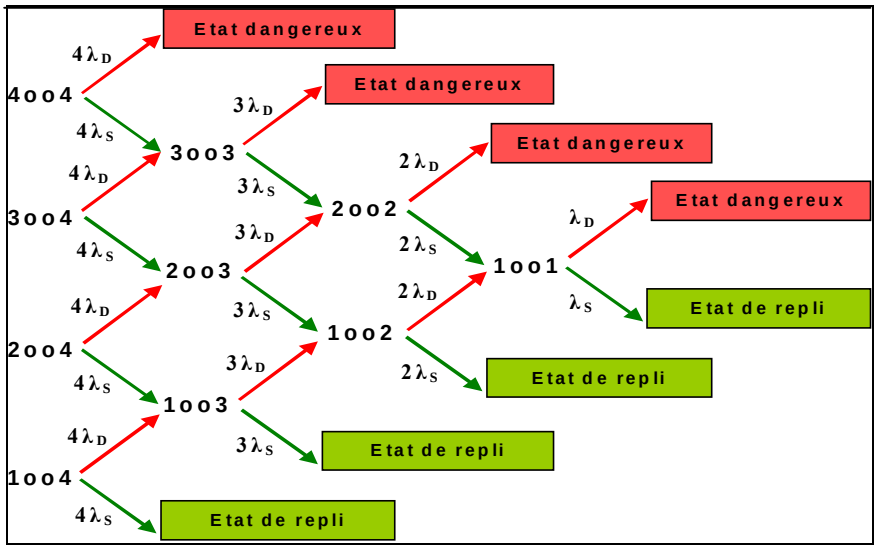

Figure 2.11 : Arborescence des architectures KooN

La lecture de cette figure montre bien que l'appréciation des performances d'une architecture *KooN* dépend du nombre de défaillances amenant soit à un état dangereux (défaillances dangereuses), soit à un état de repli sûr (défaillances sûres).

Il en ressort que la configuration optimale parmi celles présentées précédemment est l'architecture 2*oo*3, car en effet le nombre de défaillances nécessaires à l'inhibition de la fonction de sécurité est celui nécessaire à son déclenchement intempestif : *N*-*K*+1=2=*K*. Ce fait est confirmé par l'utilisation courante de cette architecture dans le domaine industriel.

Nous tenons à signaler qu'il existe des variantes des architectures *KooN* où le module de diagnostic peut couper l'alimentation de la charge en cas de détection de défaillances dangereuses, voir la figure 2.12 dans le cas d'une architecture mono-canal (1*oo*1*D*) [CHARPENTIER, 2002] [GOBLE, 1998].

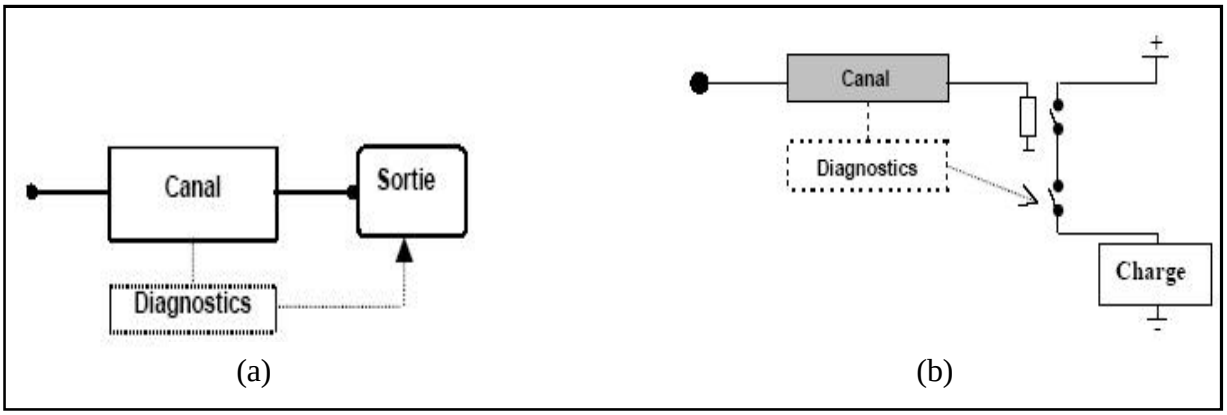

Figure 2.12 : (a) Bloc-diagramme physique et (b) schéma électrique de principe relatif à l'architecture 1*oo*1*D*

Pour terminer cette section et faciliter l'appréhension de la section suivante, en s'appuyant sur la figure 2.11, nous proposons à la figure 2.13 les différents blocs-diagramme de fiabilités, pour les défaillances dangereuses et sûres, relatifs aux architectures *KooN* classiques.

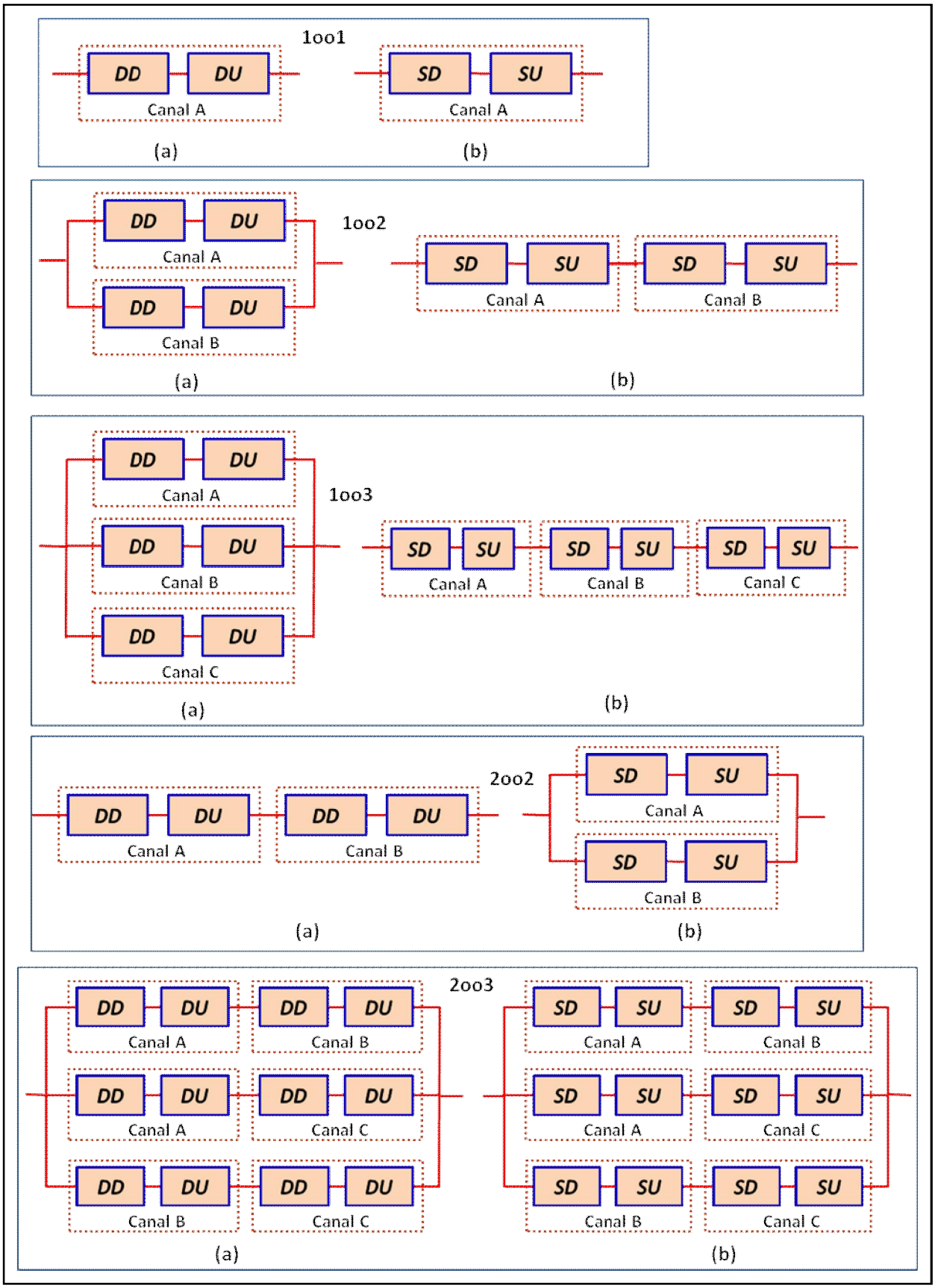

Figure 2.13 : Blocs-diagramme de fiabilité relatifs aux (a) comportement dangereux et (b) sûrs des architectures KooN classiques

2.4. Formules analytiques relatives aux performances des *SIS*

2.4.1. Introduction

La validation de la mise en place d'un système instrumenté passe, entre autres, par la comparaison de sa performance probabiliste à la mesure cible de défaillance (valeur maximale admissible définie lors de la phase d'allocation des niveaux d'intégrité de sécurité). Pour ce faire, plusieurs formulations analytiques ont été développées. Il convient de mettre en évidence que ces formulations ne sont que des approximations dont le champ applicatif et restreint. Une évaluation correcte nécessite l'utilisation des méthodes quantitatives classiques issues du domaine de la sûreté de fonctionnement : arbres des défaillances, chaînes de Markov et les Réseaux de Petri), pour plus de détail voir la référence [INNAL, 2008]. Cette deuxième alternative n'est pas celle retenue dans le cadre de ce travail.

Dans ces conditions, nous allons, dans ce qui suit, présenter les différentes formules analytiques (PFD_{moy}, *PFH*, *PFS* et *STR*) retrouvées dans la littérature :

- Formules proposées dans la CEI 61508 [CEI 61508-6, 1998] [CEI 61508-6, 2010]. Comme cette norme est orientée sécurité, seules les *PFD* et *PFH* y sont présentées.
- Formulations analytiques développées dans le cadre du travail doctoral [INNAL, 2008] et post-doctoral [DUTUIT et *al.* 2009] de Monsieur INNAL Fares. Deux approches ont été mises à profit :
  - approche markovienne approchée pour les formules donnant la PFD_{moy} et la *PFH*,
  - approche fondée sur un modèle binomial pour les formules PFD_{moy}, *PFH*, PFS_{moy} et *STR*.
- Formules exposées dans la norme américaine ISA [ISA, 2002], équivalente à la CEI 61511. Ces formules concernent les deux grandeurs d'intérêt suivant : PFD_{moy} et *STR*.
- La dernière source de formules est l'organisme norvégien SINTEF [SINTEF, 2006]. Seules les expressions des PFD_{moy}, *PFH* et *STR* y sont disponibles.

2.4.2. Formules analytiques retrouvées dans la littérature

Les performances probabilistes d'une fonction de sécurité, assurée par un *SIS* donné, sont déterminées par le calcul et la combinaison des performances de ces trois sous-systèmes (*S*, *LS* et *FE*). Cela peut être exprimé par les formules suivantes :

$$PFD_{moy}^{SIS} = PFD_{moy}^{S} + PFD_{moy}^{LS} + PFD_{moy}^{FE} \quad (2.9)$$

$$PFH_{SIS} = PFH_{S} + PFH_{LS} + PFH_{FE} \quad (2.10)$$

$$PFS_{moy}^{SIS} = PFS_{moy}^{S} + PFS_{moy}^{LS} + PFS_{moy}^{FE} \quad (2.11)$$

$$STR_{moy}^{SIS} = STR_{moy}^{S} + STR_{moy}^{LS} + STR_{moy}^{FE} \quad (2.12)$$

Bien évidemment, chacun de ces trois sous-systèmes est représenté par une architecture *KooN*.

Voyons à présent les différentes formules mathématiques retrouvées dans la littérature pour les architectures *KooN* usuelles. Chaque formule contient deux partie mutuellement exclusive : l'une concerne les défaillances indépendantes et l'autre rend compte des défaillances de cause commune (voir figure 2.14). Cette partition existe dès que *N* diffère de l'unité.

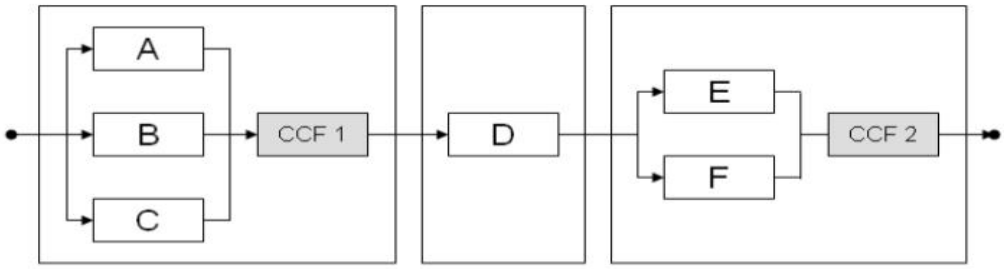

Figure 2.14 : Bloc-diagramme de fiabilité d'un SIS complet (trois capteurs (1oo3), une unité logique (1oo1), deux éléments finaux (1oo2)).

2.4.2.1. CEI 61508-6

Les différentes formules concernant la PFD_{moy} sont regroupées au tableau 2.1. Celles relatives à la *PFH* diffèrent selon les deux versions de la norme CEI 61508. Elles sont, à ce effet, données aux tableaux 2.2 [CEI 61508-6, 1998] et 2.3 [CEI 61508-6, 2009].

Architectures	PFD_{moy} **[CEI 61508-6, 2009]**
1*oo*1	$(\lambda_{DU} + \lambda_{DD})t_{CE}$
1*oo*2	$2((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
1*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^3 t_{CE} t_{GE} t_{G2E} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$
2*oo*2	$2\lambda_D t_{CE}$
2*oo*3	$6((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MRT\right)$

Avec :

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR$$

- ***MTTR*** (*mean time to restoration*) *: temps moyen de restauration d'une défaillance dangereuse détectée.*
- ***MRT*** (*mean repair time*) *: temps moyen de réparation d'une défaillance dangereuse non détectée.* La norme suppose que $MTTR \cong MRT$.
- $\beta_{DU} = \beta$; $\beta_{DD} = \beta_D$.
- La norme ne tient pas compte des défaillances de cause commune pour les architectures série, en l'occurrence la configuration 2*oo*2.

Tableau 2.1 : Formules analytiques relatives aux PFD_{moy} des architectures KooN selon la CEI 61508-6

Architectures	***PFH* [CEI 61508-6, 1998]**
1*oo*1	λ_{DU}
1*oo*2	$2\left((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\right)^2 t_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$
1*oo*3	Cette architecture n'est pas traitée dans cette version de la norme. Toutefois on peut en donner une formule mathématique en se basant sur celle de l'architecture 1*oo*2 : $6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^3\, t_{CE}\, t_{GE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$
2*oo*2	$2\lambda_{DU}$
2*oo*3	$6\left((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}\right)^2 t_{CE}+\beta_D\lambda_{DD}+\beta\lambda_{DU}$

Tableau 2.2 : Formules analytiques relatives aux PFH des architectures KooN selon la CEI 61508-6

Architectures	***PFH* [CEI 61508-6, 2009]**
1*oo*1	λ_{DU}
1*oo*2	$2((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}$
1*oo*3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})^2(1-\beta)\lambda_{DU}t_{CE}t_{GE}+\beta\lambda_{DU}$
2*oo*2	$2\lambda_{DU}$
2*oo*3	$6((1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU})(1-\beta)\lambda_{DU}t_{CE}+\beta\lambda_{DU}$

Tableau 2.3 : Formules analytiques relatives aux PFH des architectures KooN selon la CEI 61508-6

Les deux versions de la norme considèrent que la détection d'une défaillance dangereuse, pour un *SIS* non redondant (1*oo*1 et 2*oo*2) et fonctionnant en mode fortes demandes ou demande continue, conduit à la mise à l'arrêt d'urgence (activation de la fonction de sécurité) du système surveillé. Voir la figure 2.12 pour plus de clarté.

La version actuelle de la norme va au-delà de cette supposition en considérant qu'elle reste valable même pour les architectures redondantes (1*oo*2, 1*oo*3, 2*oo*3). C'est-à-dire la détection d'une défaillance dangereuse, cette dernière provoquant une panne dangereuse du *SIS*, entraine l'activation de la fonction de sécurité. Cette extension est tout à fait logique. Ceci, bien entendu, reste vrai pour les défaillances de cause commune ; d'où l'absence du terme $\beta_D\,\lambda_{DD}$ au niveau du tableau 2.3. En revanche, la modification observée au niveau des premiers termes des formules de ce même tableau restent à vérifier (ceci dépasse le champ de ce travail).

2.4.2.2. Approche SINTEF

Aux tableaux 2.4, 2.5, 2.6 et 2.7 sont présentées respectivement les différentes formules concernant les PFD_{moy}, *PFH* et *STR* [SINTEF, 2006]. La *PFS* n'est pas considérée dans l'approche SINTEF. Il convient de noter que les tableaux 2.5 et 2.6 donnés par l'organisme SINTEF dans son document [SINTEF, 2010] sont des approximations basées sur le fait de négliger, d'une part, les contributions des défaillances dangereuses détectées et, d'autre part, le facteur β devant l'unité.

Architectures	***PFD_{moy}***
1*oo*1	$\lambda_{DU}.T_1/2 + \lambda_{DD}\,.\,MTTR$
1*oo*2	$(1-\beta)^2\,\lambda_{DU}{}^2\,T_1{}^2/3 + 2(1-\beta)\lambda_{DD}.\lambda_{DU}.MTTR.T_1/2 + \beta.(\,\lambda_{DD}.MTTR + \lambda_{DU}\,T_1/2)$
1*oo*3	$0{,}3\left[\beta\,\lambda_{DD}\,MTTR + \beta\lambda_{DU}\cdot\frac{T_1}{2}\right] + \frac{1}{4}\cdot\left[(1-1{,}7\beta\,)\,\lambda_{DU}\cdot T_1\right]^3$ $+\,3\,(1-1{,}7\beta\,)\,\lambda_{DD}\cdot MTTR\cdot\beta\lambda_{DU}\cdot\frac{T_1}{2}$
2*oo*2	$(2-\beta)\,(\lambda_{DU}.T_1/2) + \beta\,\lambda_{DD}\,.\,MTTR$
2*oo*3	$2.4\beta\lambda_{DU}\tau/2 + [(1-1.7\beta)\lambda_{DU}\tau]^2 + 3(1-1.7\beta) \times\lambda_{DD}\,MTTR\beta\lambda_{DU}(\tau/2)$

- L'organisme SINTEF n'utilise pas le modèle du facteur ***β*** pour les défaillances de cause commune. Il met en œuvre un nouveau modèle, dénommé facteur ***β*** généralisé, moins pessimiste que celui utilisé par la CEI 61508.
- Le coefficient *β* lié aux défaillances de cause commune est le même pour les défaillances détectées et non détectées : $\beta_{DU} = \beta_{DD} = \beta$.

Tableau 2.4 : Formules analytiques relatives aux PFD_{moy} des architectures KooN selon SINTEF

Voting	**PFD calculation formulas**		
	Common cause contribution		**Contribution from independent failures**
1oo1	-		$\lambda_{DU}\cdot\tau/2$
1oo2	$\beta\cdot\lambda_{DU}\cdot\tau/2$	+	$[\lambda_{DU}\cdot\tau]^2/3$
2oo2	-		$2\cdot\lambda_{DU}\cdot\tau/2$
1oo3	$C_{1oo3}\cdot\beta\cdot\lambda_{DU}\cdot\tau/2$	+	$[\lambda_{DU}\cdot\tau]^3/4$
2oo3	$C_{2oo3}\cdot\beta\cdot\lambda_{DU}\cdot\tau/2$	+	$[\lambda_{DU}\cdot\tau]^2$
3oo3	-		$3\cdot\lambda_{DU}\cdot\tau/2$
1ooN; N = 2, 3,…	$C_{1ooN}\cdot\beta\cdot\lambda_{DU}\cdot\tau/2$	+	$\frac{1}{N+1}\cdot(\lambda_{DU}\cdot\tau)^N$
MooN, M<N; N = 2, 3,..	$C_{MooN}\cdot\beta\cdot\lambda_{DU}\cdot\tau/2$	+	$\frac{N!}{(N-M+2)!\cdot(M-1)!}\cdot(\lambda_{DU}\cdot\tau)^{N-M+1}$
NooN; N = 1, 2, 3, …	-		$N\cdot\lambda_{DU}\cdot\tau/2$

Tableau 2.5 : Formules analytiques simplifiées relatives aux PFD_{moy} des architectures KooN selon SINTEF

Voting	PFH calculation formulas		
	Common cause contribution		**Contribution from independent failures**
1oo1	-		λ_{DU}
1oo2	$\beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau]^2/\tau$
2oo2	-		$2 \cdot \lambda_{DU}$
1oo3	$C_{1oo3} \cdot \beta \cdot \lambda_{DU}$	+	$[\lambda_{DU} \cdot \tau]^3/\tau$
2oo3	$C_{2oo3} \cdot \beta \cdot \lambda_{DU}$	+	$3 \cdot [\lambda_{DU} \cdot \tau]^2/\tau$
3oo3	-		$3 \cdot \lambda_{DU}$
MooN, M<N; N = 2, 3, ...	$C_{MooN} \cdot \beta \cdot \lambda_{DU}$	+	$\frac{N!}{(N-M+1)!(M-1)!} \cdot \left[(\lambda_{DU} \cdot \tau)^{N-M+1}/\tau\right]$
NooN; N = 1, 2, 3, …	-		$N \cdot \lambda_{DU}$

Tableau 2.6 : Formules analytiques simplifiées relatives aux PFH des architectures KooN selon SINTEF

Architectures	***STR***
1*oo*1	λ_{SU}
1*oo*2	$2\ \lambda_{SU}$
1*oo*3	$3\ \lambda_{SU}$
2*oo*2	$\beta\ \lambda_{SU}$
2*oo*3	$C_{2oo3}\ \beta\ \lambda_{SU}$
1ooN; N= 1, 2, 3, …	$N\ \lambda_{SU}$
MooN $2 \le M \le N;\ \ N = 2, 3,...$	$C_{(N\_M+1)ooN}\ \beta\ \lambda_{SU}$

Tableau 2.7 : Formules analytiques relatives aux STR des architectures KooN selon SINTEF

Les facteurs C_{MooN} relatifs aux architectures *KooN (M=K)* sont donnés ci-après (voir tableau 2.8).

M \ N	N = 2	N = 3	N = 4	N = 5	N = 6	N = 7	N = 8
M = 1	$C_{1oo2} = 1.0$	$C_{1oo3} = 0.5$	$C_{1oo4} = 0.3$	$C_{1oo5} = 0.21$	$C_{1oo6} = 0.17$	$C_{1oo7} = 0.15$	$C_{1oo8} = 0.15$
M = 2	-	$C_{2oo3} = 2.0$	$C_{2oo4} = 1.1$	$C_{2oo5} = 0.7$	$C_{2oo6} = 0.4$	$C_{2oo7} = 0.27$	$C_{2oo8} = 0.15$
M = 3	-	-	$C_{3oo4} = 2.9$	$C_{3oo5} = 1.8$	$C_{3oo6} = 1.1$	$C_{3oo7} = 0.8$	$C_{3oo8} = 0.6$
M = 4	-	-	-	$C_{4oo5} = 3.7$	$C_{4oo6} = 2.4$	$C_{4oo7} = 1.6$	$C_{4oo8} = 1.1$
M = 5	-	-	-	-	$C_{5oo6} = 4.3$	$C_{5oo7} = 3.0$	$C_{5oo8} = 2.1$
M = 6	-	-	-	-	-	$C_{6oo7} = 4.8$	$C_{6oo8} = 3.5$
M = 7	-	-	-	-	-	-	$C_{7oo8} = 5.3$

Tableau 2.8 : C_{MooN} relatifs aux architectures KooN (M=K)

2.4.2.3. Approche ISA

La partie 2 du rapport technique ISA-TR 84.00.02 [ISA, 2002] regroupe les formules analytiques des PFD_{moy} de plusieurs architectures du type *K*oo*N* (*1oo1*, *1oo2*, 1oo3, *2oo2*, *2oo3* et *2oo4*). Ces formules incluent la contribution des défaillances systématiques. Nous n'incluons pas, dans ce qui suit et pour des raisons d'homogénéité, ces contributions dans les expressions PFD_{moy}(*K*oo*N*) données par l'ISA, d'autant plus, que dans tous les cas d'application présentés dans le document précité, les défaillances systématiques sont considérées comme négligeables (voir tableau 2.9).

Comme l'ISA ne traite que la faible demande, les *PFH* n'y sont pas données. C'est également le cas pour les PFS_{moy}. En revanche, les expressions relatives aux *STR* y sont disponibles et rappelées au tableau 2.10.

Architectures	$\boldsymbol{PFD_{moy}}$
1*oo*1	$\lambda_{DU} \cdot \frac{Ti}{2} + \lambda_F^D \cdot \frac{Ti}{2} \approx \lambda_{DU} \cdot \frac{Ti}{2}$
1*oo*2	$\left[\lambda_{DU}^2 \cdot \frac{Ti^2}{3}\right] + \left[\lambda_{DU} \cdot \lambda_{DD} \cdot MTTR \cdot Ti\right] + \beta \lambda_{DU} \cdot \frac{Ti}{2}$
1*oo*3	$\left[\lambda_{DU}^3 \cdot \frac{Ti^3}{4}\right] + \left[\lambda_{DU}^2 \cdot \lambda_{DD} \cdot MTTR \cdot Ti^2\right] + \beta \lambda_{DU} \cdot \frac{Ti}{2}$
2*oo*2	$\left[\lambda_{DU} \cdot Ti\right] + \left[\beta \lambda_{DU} \cdot Ti\right]$
2*oo*3	$\left[\lambda_{DU}^2 \cdot Ti^2\right] + \left[3\lambda_{DU} \cdot \lambda_{DD} \cdot MTTR \cdot Ti\right] + \beta \lambda_{DU} \cdot \frac{Ti}{2}$

- λ_F^D : Taux des défaillances dangereuses systématiques.
- $Ti = T_1$.
- Il est supposé qu'en cas de défaillance dangereuse détectée, le SIS amène le procédé dans un état sûr ou qu'un opérateur le sécurise d'une manière immédiate et parfaite.
- La valeur du coefficient β du modèle de même nom, utilisé pour traité des défaillances de cause commune, est négligeable devant l'unité.
- Les formules données par l'ISA représentent des approximations optimistes de celles de la norme CEI 61508.

Tableau 2.9 : Formules analytiques relatives aux PFD_{moy} des architectures KooN selon l'ISA

Nous pensons que les formules analytiques relatives aux PFD_{moy} des architectures 1*oo*1, 1*oo*2 et 1*oo*3 sont fausses. En effet, les architectures 1*ooN* (avec $N \geq 2$) sont connues pour être robustes vis-à-vis des défaillances dangereuses notamment détectées. Pourquoi alors les mettre à l'arrêt, en état sûr, dès la première défaillance dangereuse détectée? A contrario pourquoi tolérer une défaillance dangereuse détectée au sein d'une architecture 2*oo*2 qui se retrouve dans un état dangereux dès l'occurrence d'une telle défaillance?

Architectures	***STR***
1*oo*1	$\lambda_S + \lambda_{DD}$
1*oo*2	$2 \cdot \left[\lambda_S + \lambda_{DD} \right] + \beta (\lambda_S + \lambda_{DD})$
1*oo*3	$3 \cdot \left[\lambda_S + \lambda_{DD} \right] + \beta (\lambda_S + \lambda_{DD})$
2*oo*2	$2 \cdot \lambda_S \left[\lambda_S + \lambda_{DD} \right] \cdot MTTR + \beta (\lambda_S + \lambda_{DD})$
2*oo*3	$6 \cdot \lambda_S \left[\lambda_S + \lambda_{DD} \right] \cdot MTTR + \beta (\lambda_S + \lambda_{DD})$

- $\beta = \beta_{SU} = 2\,\beta_{SD} = \beta << 1$.
- Les défaillances sûres, quelles qu'elles soient, sont supposées détectées en ligne !
- Les défaillances dangereuses détectées sont intégrées aux défaillances sûres quand elles amènent le canal concerné d'un système redondant ou le système lui-même, quand il n'est pas redondant, dans un état sûr. Si ce n'est pas le cas, ces défaillances dangereuses détectées ne sont pas prises en compte.

Tableau 2.10 : Formules analytiques relatives aux STR des architectures KooN selon l'ISA

2.4.2.4. Travail doctoral et post-doctoral de Monsieur INNAL Fares

Comme nous l'avons mentionné au paragraphe 2.4.1, ces travaux concernent les quatre grandeurs probabilistes. Nous résumant dans ce qui suit leurs formulations analytiques, fondées sur deux approches différentes : markovienne approchée et modèle binomial.

- ***Approche markovienne :*** le principe de cette première approche se résume dans le schéma ci-après [INNAL, 2011]. Seules les PFD_{moy} et *PFH* ont été établies (voir tableaux 2.11 et 2.12).

1. Approximer le modèle markovien multi-phases (exact) par un modèle continu (approché), sans prise en compte des DCC
2. Déterminer les taux de retour des états de panne
3. Calculer les probabilités asymptotiques (modèle continu)
4. Calculer la *MDT*
5. Calculer la fréquence de défaillance asymptotique : $w = 1/MTBF = PFH$
6. Déduire la *PFD* : $PFD = MDT/MTBF$
7. Répéter les étapes 1 à 6 pour les défaillances de cause commune (DCC)
8. $PFD_{kooN} = PFD_{sans\ DCC} + PFD_{DCC}$
9. $PFH_{KooN} = PFH_{sans\ DCC} + PFH_{DCC}$

Figure 2.15 : Procédure d'obtention des PFD_{moy} et PFH des architectures KooN basée sur une modélisation markovienne « approchée »

Architectures	***PFD_{moy}***
1oo1	$\lambda_{DU}.(T_1/2 + MTTR) + \lambda_{DD} . MTTR$
1oo2	$2\lambda_D^2\left[\frac{(1-\beta)\ \lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{(1-\beta_D)\ \lambda_{DD}}{\lambda_D}MTTR\right]$ $\times\left[\frac{\lambda_{DD}}{\lambda_D}MTTR\ +\frac{\lambda_{DU}}{\lambda_D}(T_1/3+MTTR\ )\right]$ $+\beta_D\lambda_{DD}MTTR+\beta\ \lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$
1oo3	$6\lambda_D[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]\cdot\left[(1-\beta_D)\lambda_{DD}MTTR+(1-\beta)\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)\right]$ $\times\left[\frac{(1-\beta_D)\ \lambda_{DD}MTTR}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}+\frac{(1-\beta)\lambda_{DU}}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}\left(\frac{T_1}{3}+MTTR\right)\right]$ $\times\left[\frac{\lambda_{DD}MTTR}{\lambda_D}+\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4}+MTTR\right)\right]$ $+3\ [\beta_D\lambda_{DD}+\beta\lambda_{DU}]\left[(1-\beta_D)\lambda_{DD}MTTR+(1-\beta)\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)\right]$ $\times\left[\frac{\beta_D\lambda_{DD}MTTR}{\beta_D\lambda_{DD}+\beta\ \lambda_{DU}}+\frac{\beta\ \lambda_{DU}}{\beta_D\lambda_{DD}+\beta\ \lambda_{DU}}\left(\frac{T_1}{3}+MTTR\right)\right]$ $+\beta_D\lambda_{DD}MTTR+\beta\ \lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$

2oo2	$2\left[(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}\right]$ $\times\left[\frac{(1-\beta)\ \lambda_{DU}}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}\left(\frac{T_1}{2}+MTTR\right)+\frac{(1-\beta_D)\ \lambda_{DD}}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}MTTR\right]$ $+\beta_D\lambda_{DD}MTTR+\beta\ \lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$
2oo3	$3[(2-\beta_D).\lambda_{DD}+(2-\beta).\lambda_{DU}]\ [(1-\beta_D).\lambda_{DD}.MTTR+(1-\beta).\lambda_{DU}\ (T_1/2+MTTR)]$ $\times\left[\frac{(2-\beta_D)\lambda_{DD}}{(2-\beta_D)\lambda_{DD}+(2-\beta)\lambda_{DU}}.MTTR+\frac{(2-\beta)\lambda_{DU}.[T_1/3+MTTR]}{(2-\beta_D)\lambda_{DD}+(2-\beta)\lambda_{DU}}\right]$ $+\beta_D\lambda_{DD}MTTR+\beta\ \lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)$

Tableau 2.11 : Formules analytiques relatives aux PFD_{moy} des architectures KooN obtenues via une approche markovienne approchée

Architectures	***PFH***
1oo1	$\lambda_{DU}+\lambda_{DD}$
1oo2	$2\lambda_D^2\left[\frac{(1-\beta)\ \lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right)+\frac{(1-\beta_D)\ \lambda_{DD}}{\lambda_D}MTTR\right]$ $+\beta_D\lambda_{DD}+\beta\ \lambda_{DU}$
1oo3	$6\lambda_D[(1-\beta_D)\lambda_{DD}+(1-\beta)\lambda_{DU}]\cdot\left[(1-\beta_D)\lambda_{DD}MTTR+(1-\beta)\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)\right]$ $\times\left[\frac{(1-\beta_D)\ \lambda_{DD}MTTR}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}+\frac{(1-\beta)\lambda_{DU}}{(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}}\left(\frac{T_1}{3}+MTTR\right)\right]$ $+3\ [\beta_D\lambda_{DD}+\beta\lambda_{DU}]\left[(1-\beta_D)\lambda_{DD}MTTR+(1-\beta)\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)\right]$ $+\beta_D\lambda_{DD}+\beta\ \lambda_{DU}$
2oo2	$2\left[(1-\beta_D)\ \lambda_{DD}+(1-\beta)\lambda_{DU}\right]+\beta_D\lambda_{DD}+\beta\ \lambda_{DU}$
2oo3	$3[(2-\beta_D).\lambda_{DD}+(2-\beta).\lambda_{DU}]\ [(1-\beta_D).\lambda_{DD}.MTTR+(1-\beta).\lambda_{DU}\ (T_1/2+MTTR)]$ $+\beta_D\ \lambda_{DD}+\beta\ \lambda_{DU}$

Tableau 2.12: Formules analytiques relatives aux PFH des architectures KooN obtenues via une approche markovienne approchée

Si l'on faisait l'hypothèse de la mise en sécurité de l'installation surveillée en cas de défaillances dangereuses détectées, il conviendrait de retrancher les termes relatifs à la contribution des défaillances détectées de cause commune, en l'occurrence $\beta_D\ \lambda_{DD} MTTR$ et $\beta_D\ \lambda_{DD}$, des formules présentées aux tableaux 2.11 et 2.12.

On peut facilement remarquer que les formules données dans la norme CEI 61508 ne sont que des approximations optimistes des formules trouvées en suivant l'approche markovienne.

- ***Approche binomiale :*** elle s'est appuyée sur les formules suivantes :

$$PFD_{moy}(KooN) = A_N^{N-K+1}\ \lambda_{Dind}^{N-K+1} \prod_{i\ =\ 1}^{N-K+1} MDT_{1ooi} + \beta\ \lambda_{DU} \cdot \left(\frac{T1}{2} + MTTR\right) + \beta_D\ \lambda_{DD} \cdot MTTR \quad (2.13)$$

$$PFH\ (KooN) = A_N^{N-K+1}\ \lambda_{Dind}^{N-K+1} \prod_{i\ =\ 1}^{N-K} MDT_{1ooi} + \beta\ \lambda_{DU} + \beta_D\ \lambda_{DD} \quad (2.14)$$

$$PFS_{moy}\ (KooN) \approx A_N^K \cdot \lambda_{Sind}^K \cdot \left[\prod_{i=1}^{K-1} MDTS_i\right] \cdot MTTR_{sd} + \left[\beta\ \lambda_{SU} + \beta_D\ \lambda_{SD}\right] \cdot MTTR_{sd} \quad (2.15)$$

$$STR(KooN) \approx A_N^K \cdot \lambda_{Sind}^K \cdot \left[\prod_{i=1}^{K-1} MDTS_i\right] + \left[\beta\ \lambda_{SU} + \beta_D\ \lambda_{SD}\right] \quad (2.16)$$

Avec :

$$A_N^{N-K+1} = \frac{N!}{(K-1)!}$$

$$\lambda_D = \lambda_{DU} + \lambda_{DD}$$

$$\lambda_{Dind} = (1-\beta)\ \lambda_{DU} + (1-\beta_D)\ \lambda_{DD}$$

$$\lambda_S = \lambda_{SU} + \lambda_{SD}$$

$$\lambda_{Sind} = (1-\beta_{SU})\ \lambda_{SU} + (1-\beta_{SD})\ \lambda_{SD}$$

$$MDT_{1ooi} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{i+1} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR$$

$$MDTS_{1ooi} = \frac{\lambda_{SU}}{\lambda_S} \cdot \left(\frac{T_1}{i+1} + MTTR_{SD}\right) + \frac{\lambda_{SD}}{\lambda_S} \cdot MTTR_{SD}$$

$MTTR_{SD}$: durée moyenne de réparation d'une défaillance sûre (détectée).

$MTTR_{sd}$: durée moyenne d'indisponibilité de l'*EUC* suite à un déclenchement intempestif du *SIS*.

Pour une architecture 1*oo*1, au niveau de la formule 2.13, on doit supprimer la contribution de cause commune et mettre $\lambda_{Dind} = \lambda_D = \lambda_{DU} + \lambda_{DD}$.

Dans ces conditions, les formules 2.13 et 2.14 généralisent les formules données dans la version précédente de la CEI 61508 [CEI 61508-6, 1998], excepté l'architecture 2*oo*2 (car la norme ne considère pas les causes commune pour les architectures séries).

Sont présentés aux tableaux 2.13 et 2.14 deux échantillons de résultats relatifs respectivement aux architectures 1*oo*2 et 2*oo*3, afin de donner des éléments de comparaison des différentes formules précédentes. Le jeu de données utilisé à cet effet est : T_1 = 1 an (8760 h), λ = 5E-5h^{-1}, λ_s = 2.5E-5h^{-1}, B_{SD} = (B_{DD}= B_D) = (B_{DU} =*B)* /2=B_{SU}/2, *MTTR*=$MTTR_{SD}$ = 8h, $MTTR_{sd}$ = 24h.

Il importe de signaler que les résultats relatifs aux *PFS* et *STR* issus de l'approche markovienne sont obtenus via les formules analytiques établies dans la suite de ce chapitre (*cf.* section 2.4.3).

Littérature	DC (%)	β (%)	PFD	PFH	PFS	STR
CEI 61508 (ancienne version)	0	10	2,40E-02	6,90E-06		
		20	3,20E-02	8,50E-06		
	60	10	6,00E-03	3,70E-06		
		20	1,20E-02	5,10E-05		
	90	10	1,30E-03	1,90E-06		
		20	2,30E-03	3,20E-06		
SINTEF	0	10	2,39E-02	7,97E-06		5E-5
		20	3,21E-02	10,47E-6		5E-5
	60	10	6,47E-03	1,87E-06		2E-5
		20	1,04E-02	2,87E-06		2E-5
	90	10	1,24E-03	3,04E-07		5E-6
		20	2,33E-03	5,54E-07		5E-6
ISA	0	10	1,10E-02			5,25E-05
		20	2,19E-02			5,50E-05
	60	10	4,38E-03			7,35E-05
		20	8,76E-03			7,00E-05
	90	10	1,10E-03			9,98E-05
		20	2,19E-03			1,04E-04
Approche Binomiale	0	10	2,40E-02	6,90E-06	1,14E-03	4,75E-05
		20	3,20E-02	8,50E-06	1,08E-03	4,50E-05
	60	10	6,00E-03	3,70E-06	1,16E-03	4,83E-05
		20	1,20E-02	5,10E-05	1,12E-03	4,65E-05
	90	10	1,30E-03	1,90E-06	1,17E-03	4,86E-05
		20	2,30E-03	3,20E-06	1,13E-03	4,73E-05
Approche markovienne	0	10	2,40E-02	6,94E-06	1,25E-03	5,23E-05
		20	3,22E-02	8,51E-06	1,06E-03	4,40E-05
	60	10	6,63E-03	3,65E-06	1,15E-03	4,80E-05
		20	1,07E-02	5,13E-06	1,08E-03	4,50E-05
	90	10	1,25E-03	1,87E-06	1,16E-03	4,82E-05
		20	2,33E-03	3,19E-06	1,12E-03	4,68E-05

Tableau 2.13 : Résultats numériques relatifs aux PFD_{moy} /PFH /PFS/STR de l'architecture 1oo2

Littérature	*DC (%)*	*β (%)*	*PFD*	*PFH*	*PFS*	*STR*
CEI 61508 (ancienne version)	*0*	*10*	5,00E-02	>1 E -5		
		20	5,30E-02	>1 E -5		
	60	*10*	1,10E-02	7,46E-06		
		20	1,50E-02	8,38E-06		
	90	*10*	1,60E-03	2,87E-06		
		20	2,60E-03	4,07E-06		
SINTEF	*0*	*10*	6,98E-02	2,14E-05		5E-6
		20	9,17E-02	2,64E-05		1E-5
	60	*10*	1,55E-02	4,62E-06		2E-6
		20	2,51E-02	6,62E-06		4E-6
	90	*10*	2,66E-03	6,6E-07		5E-7
		20	4,85E-03	1,16E-06		1E-6
ISA	*0*	*10*	5,89E-02			3,60E-03
		20	6,99E-02			3,61E-03
	60	*10*	1,21E-02			5,76E-03
		20	1,65E-02			5,77E-03
	90	*10*	1,59E-03			6,84E-03
		20	2,68E-03			6,85E-03
Approche Binomiale	*0*	*10*	5,00E-02	1,00E-05	3,80E-04	1,58E-05
		20	5,30E-02	1,00E-05	3,73E-04	1,55E-05
	60	*10*	1,10E-02	7,46E-06	1,79E-04	7,45E-06
		20	1,50E-02	8,38E-06	2,01E-04	8,38E-06
	90	*10*	1,60E-03	2,87E-06	6,83E-05	2,84E-06
		20	2,60E-03	4,07E-06	9,73E-05	4,05E-06
Approche markovienne	*0*	*10*	5,22E-02	1,58E-05	3,52E-04	1,47E-05
		20	5,66E-02	1,55E-05	3,74E-04	1,56E-05
	60	*10*	1,10E-02	7,46E-06	1,73E-04	7,20E-06
		20	1,44E-02	8,38E-06	1,87E-04	7,77E-06
	90	*10*	1,54E-03	2,87E-06	6,44E-05	2,68E-06
		20	2,57E-03	4,07E-06	9,11E-05	3,80E-06

Tableau 2.14 : Résultats numériques relatifs aux PFD_{moy} /PFH /PFS/STR de l'architecture 2oo3

La lecture des tableaux 2.13 et 2.14 nous permet de constater que les différentes sources bibliographiques donnent des résultats plus ou moins distincts. Ceci est imputable aux hypothèses utilisées par chacune d'elles. Un bon accord est toutefois constaté entre les résultats fournis par les approches binomiales et markovienne.

2.4.3. Formulation analytique des *PFS* et *STR* des architectures *KooN* à l'aide des chaînes de Markov

Pour établir cette formulation analytique, nous allons suivre la procédure décrite à la figure 2.16, mais cette fois-ci pour les défaillances sûres. A ce titre, nous allons mettre à profit le logiciel GRIF développé par la société française TOTAL [GRIF, 2011].

2.4.3.1. Architecture 1*oo*1

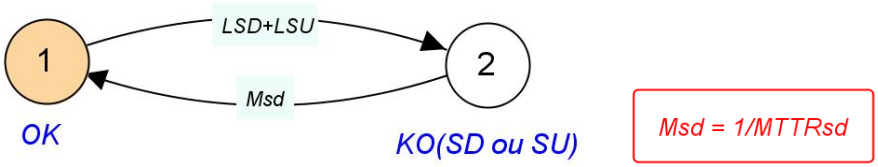

Figure 2.16 : Modélisation markovienne des défaillances sûres de l'architecture 1*oo*1

L'écriture matricielle de la chaîne de Markov de l'architecture 1*oo*1 en régime stationnaire est la suivante :

$$\begin{bmatrix}0\\0\end{bmatrix}=\begin{bmatrix}-(\lambda_{SD}+\lambda_{SU}) & \mu_{sd}\\ (\lambda_{SD}+\lambda_{SU}) & -\mu_{sd}\end{bmatrix}\begin{bmatrix}P_1(\infty)\\P_2(\infty)\end{bmatrix}\Rightarrow \left.\begin{array}{rcl} P_1(\infty) & = & \dfrac{\mu_{sd}}{\mu_{sd}+\lambda_{SD}+\lambda_{SU}}\approx 1,\ \text{puisque}\ \mu_{sd} >> \lambda_{SD}+\lambda_{SU}\\ P_2(\infty) & = & \dfrac{\lambda_{SD}+\lambda_{SU}}{\mu_{sd}+\lambda_{SD}+\lambda_{SU}}\approx \dfrac{\lambda_{SD}+\lambda_{SU}}{\mu_{sd}}\end{array}\right\} \quad (2.17)$$

La PFS_{moy} peut être approchée par la probabilité asymptotique de l'état 2. On peut alors écrire :

$$PFS_{moy}^{1oo1}\approx P_2(\infty)\approx\frac{\lambda_{SD}+\lambda_{SU}}{\mu_{sd}}=(\lambda_{SD}+\lambda_{SU})\cdot MTTR_{sd} \quad (2.18)$$

Le *STR* peut être obtenu par la mise en œuvre de la méthode des états de marche critique [PAGES et *al*, 1980] :

$$STR_{1oo1}\approx P_1(\infty)\cdot(\lambda_{SD}+\lambda_{SU})\approx(\lambda_{SD}+\lambda_{SU}) \quad (2.19)$$

On peut également obtenir directement la formule (2.19) en se basant sur la relation générale suivante [INNAL, 2008] [DUTUIT et *al.* 2009] :

$$STR_{KooN}=\frac{PFS_{moy}^{KooN}}{MTTR_{sd}} \quad (2.20)$$

Le tableau 2.15 regroupe quelques résultats obtenus, d'une part, directement à l'aide du logiciel GRIF, et en utilisant les formules (2.18) et (2.19), d'autre part. Pour cela, les données sont : λ_s = 2.5E-5h^{-1} ; $MTTR_{sd}$ = 24h.

Approches	DC_S %	PFS	STR (h^{-1})
GRIF	0	5.9964E-4	2.4985E-5
	60	5.9964E-4	2.4985E-5
	90	5.9964E-4	2.4985E-5
Formules	0	6E-4	2.5E-5
	60	6E-4	2.5E-5
	90	6E-4	2.5E-5

Tableau 2.15 : Résultats numériques relatifs aux PFS/STR de l'architecture 1oo1

2.4.3.2. Architecture 1oo2

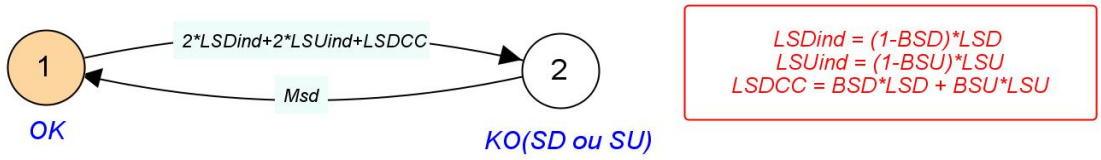

Figure 2.17 : Modélisation markovienne des défaillances sûres de l'architecture 1oo2

$$\begin{bmatrix} -2(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC} & \mu_{sd} \\ 2(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC} & -\mu_{sd} \end{bmatrix} \begin{bmatrix} P_1(\infty) \\ P_2(\infty) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \quad \Rightarrow$$

$$\left.\begin{aligned} P_1(\infty) &= \frac{\mu_{sd}}{\mu_{sd}+2\cdot(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC}} \approx 1 \\ P_2(\infty) &= \frac{2\cdot(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC}}{\mu_{sd}+2\cdot(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC}} \approx \frac{2\cdot(\lambda_{SDind}+\lambda_{SUind})+\lambda_{SDCC}}{\mu_{sd}} \end{aligned}\right\}$$

(2.21)

Comme dans le cas précédent, la *PFS* et le *STR* se déduisent ainsi :

$$PFS_{moy}^{1oo2} \approx P_2(\infty) \approx \left[2\cdot\left((1-\beta_{SD})\lambda_{SD}+(1-\beta_{SU})\lambda_{SU}\right)+\beta_{SD}\lambda_{SD}+\beta_{SU}\lambda_{SU}\right]\cdot MTTR_{sd} \qquad (2.22)$$

$$STR_{1oo2} \approx 2\cdot\left((1-\beta_{SD})\lambda_{SD}+(1-\beta_{SU})\lambda_{SU}\right)+\beta_{SD}\lambda_{SD}+\beta_{SU}\lambda_{SU} \qquad (2.23)$$

Le tableau 2.16 regroupe les valeurs numériques relatives à la PFS_{moy} et *STR* de l'architecture 1oo2. Les données sont : λ_s = 2.5E-5h^{-1} ; $MTTR_{sd}$ = 24h ; $\beta_{SU} = 2*\beta_{SD}$= 0.2.

Approches	DC_S %	PFS	STR (h^{-1})
GRIF	0	1.0788E-3	4.495E-5
	60	1.1147E-3	4.6448E-5
	90	1.1339E-3	4.7246E-5
Formules	0	1.08E-3	4.5E-5
	60	1.116E-3	4.65E-5
	90	1.1352E-3	4.73E-5

Tableau 2.16 : Résultats numériques relatifs aux PFS/STR de l'architecture 1oo2

2.4.3.3. Architecture 1oo3

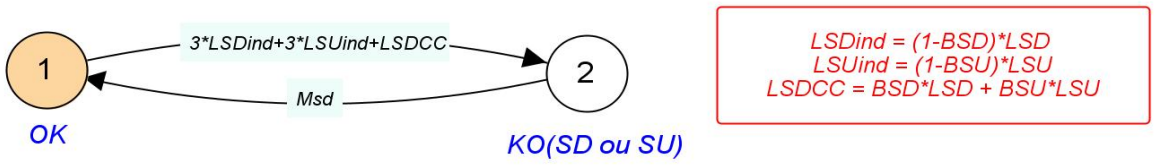

Figure 2.18 : Modélisation markovienne des défaillances sûres de l'architecture 1oo3

D'une manière analogue à l'architecture 1oo2, on peut établir pour l'architecture 1oo3 :

$$PFS_{moy}^{1oo3} \approx P_2(\infty) \approx \left[3\cdot\left((1-\beta_{SD})\,\lambda_{SD}+(1-\beta_{SU})\,\lambda_{SU}\right)+\beta_{SD}\lambda_{SD}+\beta_{SU}\lambda_{SU}\right]\cdot MTTR_{sd} \quad (2.24)$$

$$STR_{1oo3} \approx 3\cdot\left((1-\beta_{SD})\,\lambda_{SD}+(1-\beta_{SU})\,\lambda_{SU}\right)+\beta_{SD}\lambda_{SD}+\beta_{SU}\lambda_{SU} \quad (2.25)$$

Pour le même jeu de paramètres précédent, les résultats numériques relatifs à l'architecture 1oo3 sont donnés au tableau ci-dessous.

Approches	DC_S %	PFS	STR (h^{-1})
GRIF	0	1.5575E-3	6.4898E-5
	60	1.6293E-3	6.7889E-5
	90	1.6652E-3	6.9384E-5
Formules	0	1.56E-3	6.5E-5
	60	1.63E-3	6.8E-5
	90	1.67E-3	6.95E-5

Tableau 2.17 : Résultats numériques relatifs aux PFS/STR de l'architecture 1oo3

Pour les architectures 1oo1, 1oo2 et 1oo3, où une seule défaillance sûre entraine l'arrêt intempestif du système surveillé, les résultats numériques retrouvés directement par le logiciel GRIF (par le traitement des graphes markoviens) et celles obtenus via les formules analytiques, déduites de ces graphes, sont très proches les uns aux autres. Les formules analytiques donnent toutefois des résultats légèrement pessimistes.

2.4.3.4. Architecture 2oo2

L'exécution intempestive de la fonction de sécurité nécessite l'occurrence de deux défaillances sûres. Il est donc claire qu'une seule défaillance sûre non détectée (λ_{SU}) reste cachée jusqu'au prochain test périodique (T_1). Ce fait ne pouvant être modélisé correctement avec un graphe markovien classique, l'usage d'un modèle markovien multi-phase s'impose (voir figure 2.19) [INNAL, 2008].

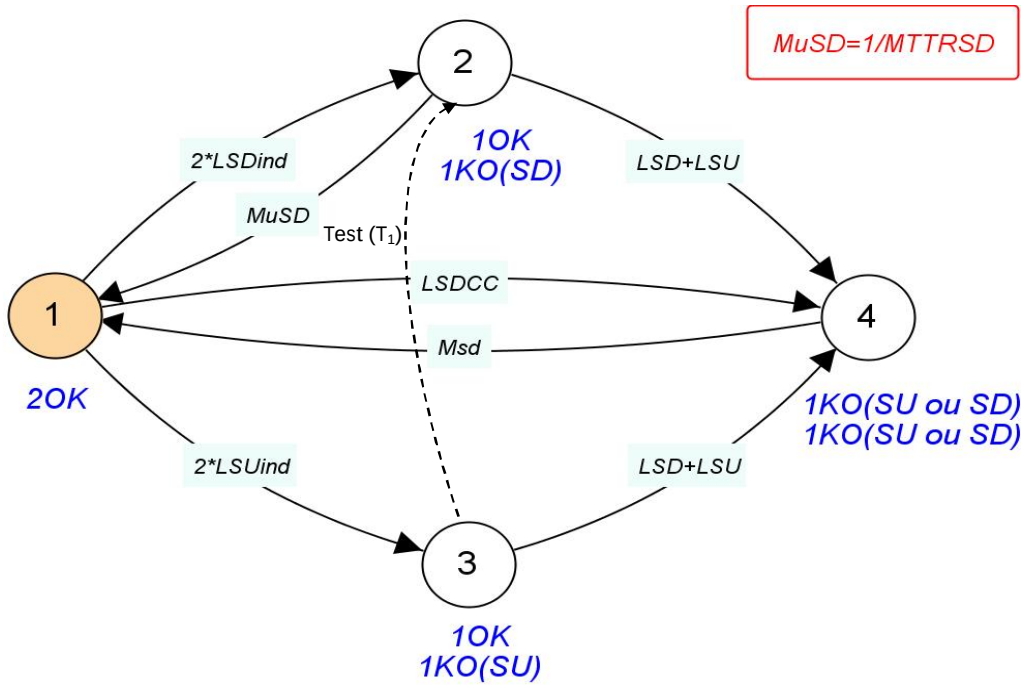

Figure 2.19 : Modélisation markovienne multi-phases des défaillances sûres de l'architecture 2oo2

Pour extraire de ce modèle les formules analytiques relatives aux PFS_{moy} et *STR*, il est nécessaire de l'approximer par un modèle markovien classique (voir figure 2.20).

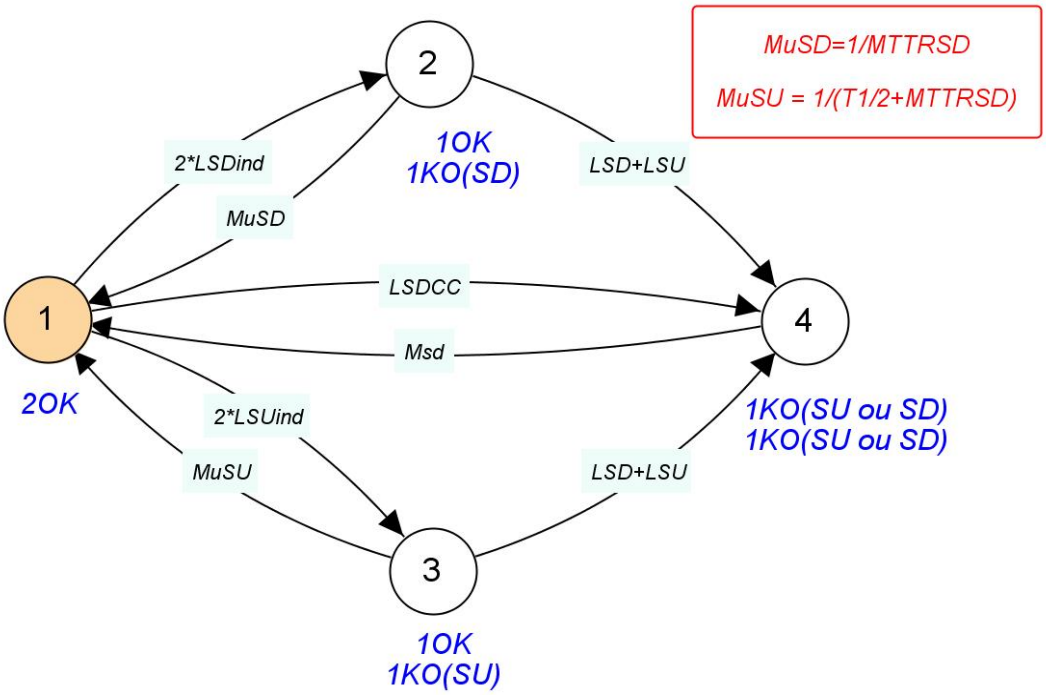

Figure 2.20 : Modélisation markovienne approchée des défaillances sûres de l'architecture 2oo2

L'exploitation de ce dernier modèle permet les développements suivants :

$$\left.\begin{aligned}
&P_1(\infty)=1-P_2(\infty)+P_3(\infty)+P_4(\infty)\approx 1\\
&P_2(\infty)=P_1(\infty).\frac{2\lambda_{SDind}}{\mu_{SD}+\lambda_{SD}+\lambda_{SU}}\approx\frac{2\lambda_{SDind}}{\mu_{SD}}=2\cdot(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}\\
&P_3(\infty)=P_1(\infty).\frac{2\lambda_{SUind}}{\mu_{SU}+\lambda_{SD}+\lambda_{SU}}\approx\frac{2\lambda_{SUind}}{\mu_{SU}}=2\cdot(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\\
&P_4(\infty)=P_1(\infty)\cdot\frac{\lambda_{SDCC}}{\mu_{sd}}+\left[P_2(\infty)+P_3(\infty)\right].\left[\frac{\lambda_{SD}+\lambda_{SU}}{\mu_{sd}}\right]\\
&\quad\approx 2\cdot(\lambda_{SD}+\lambda_{SU})\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right]\cdot MTTR_{sd}\\
&\qquad\qquad+\lambda_{SDCC}\cdot MTTR_{sd}
\end{aligned}\right\}\quad(2.26)$$

On obtient finalement :

$$PFS_{moy}^{2oo2}\approx 2\cdot(\lambda_{SD}+\lambda_{SU})\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right]\cdot MTTR_{sd}+\lambda_{SDCC}\cdot MTTR_{sd}\quad(2.27)$$

$$STR_{2oo2}\approx 2\cdot(\lambda_{SD}+\lambda_{SU})\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right]+\lambda_{SDCC}\quad(2.28)$$

Les résultats numériques relatifs à l'architecture 2*oo*2, obtenus via le logiciel GRIF (modèles multi-phases (*MMP*) et approché (*MA*)) de même que les formules analytiques, sont donnés au tableau ci-dessous.

Approches	***DC$_S$ %***	***PFS***	***STR (h^{-1})***
GRIF Multi-phases	***0***	1.902E-4	7.926E-6
	60	1.163E-4	4.847E-6
	90	7.480E-5	3.116E-6
GRIF Markov approché	***0***	1.855E-4	7.729E-6
	60	1.148E-4	4.783E-6
	90	7.447E-5	3.103E-6
Formules	***0***	2,25E-04	9,38E-06
	60	1,26E-04	5,26E-06
	90	7,65E-05	3,19E-06

Tableau 2.18 : Résultats numériques relatifs aux PFS/STR de l'architecture 2*oo*2

Les différentes courbes concernant les indicateurs *PFS* et *STR* obtenues à l'aide du logiciel GRIF sont exposées à la figure 2.21 (pour *DC*= 60%).

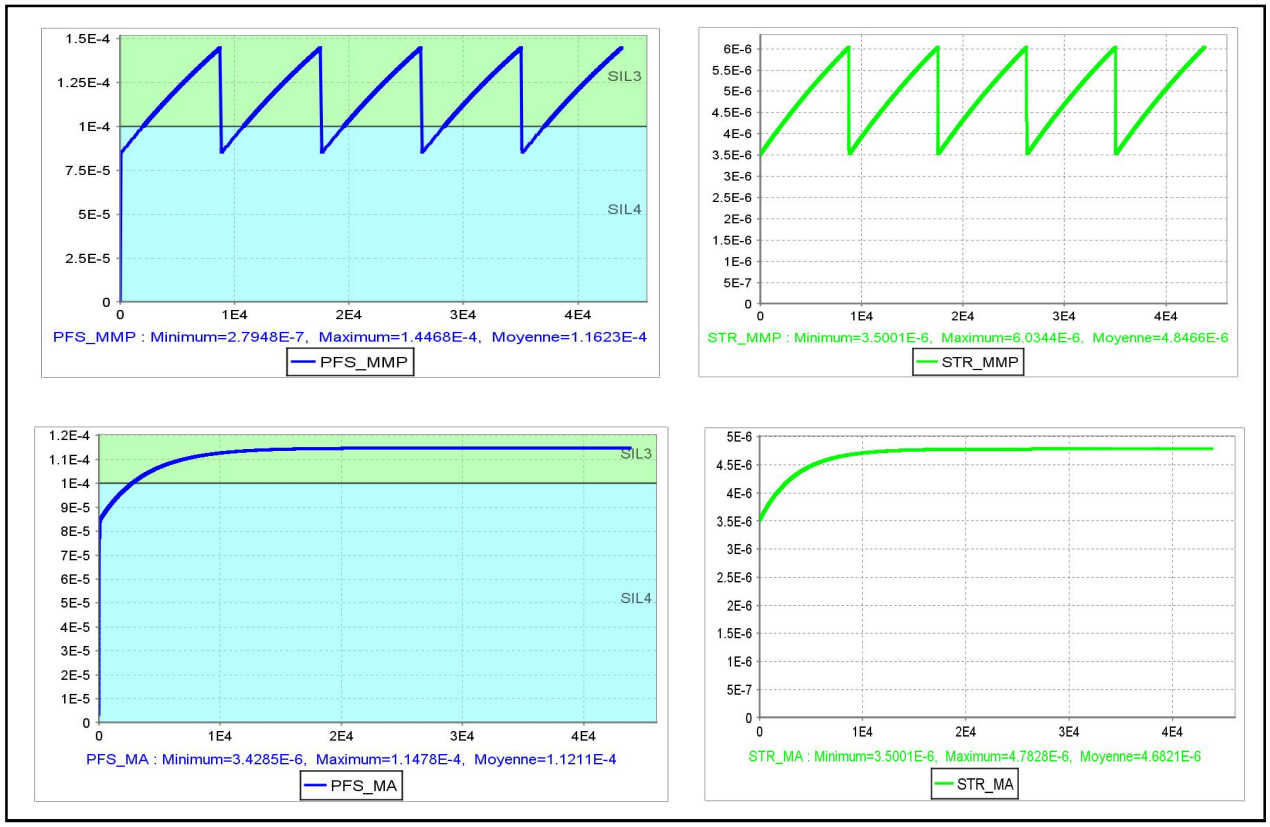

Figure 2.21 : Courbes relatives aux PFS/STR de l'architecture 2*oo*2

2.4.3.5. Architecture 2*oo*3

Le comportement dysfonctionnel de l'architecture 2*oo*3, vis-à-vis des défaillances sûres, est similaire à celui de l'architecture 2*oo*2, comme on peut le constater aux niveaux des figures 2.22 et 2.23.

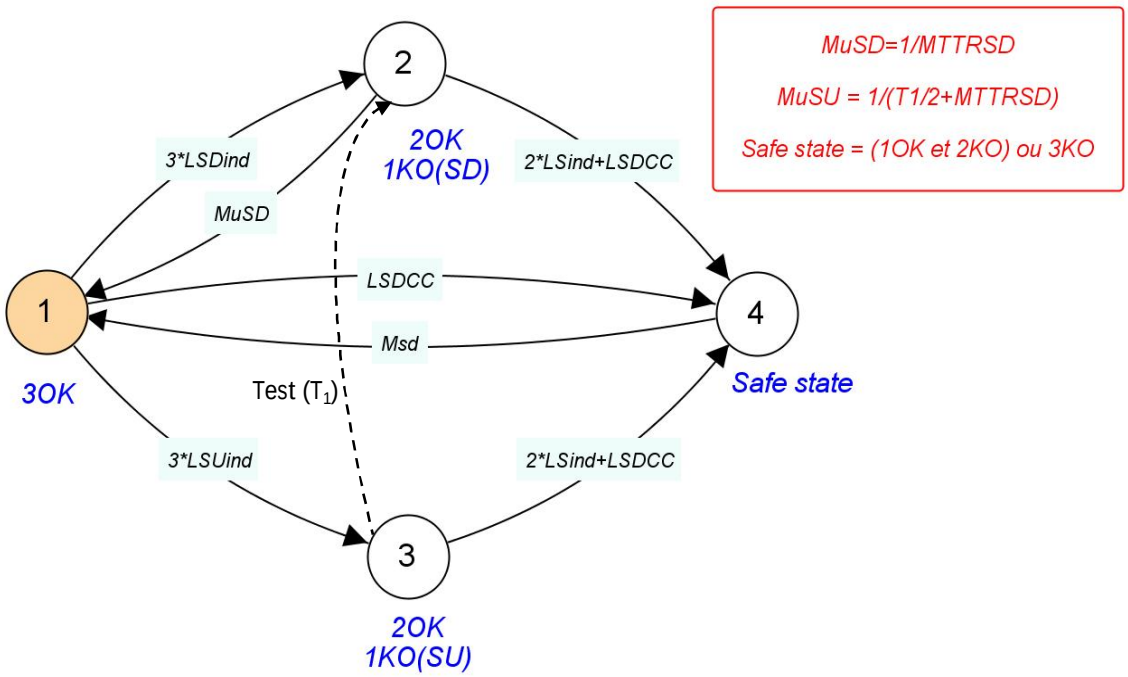

Figure 2.22: Modélisation markovienne multi-phases des défaillances sûres de l'architecture 1*oo*3

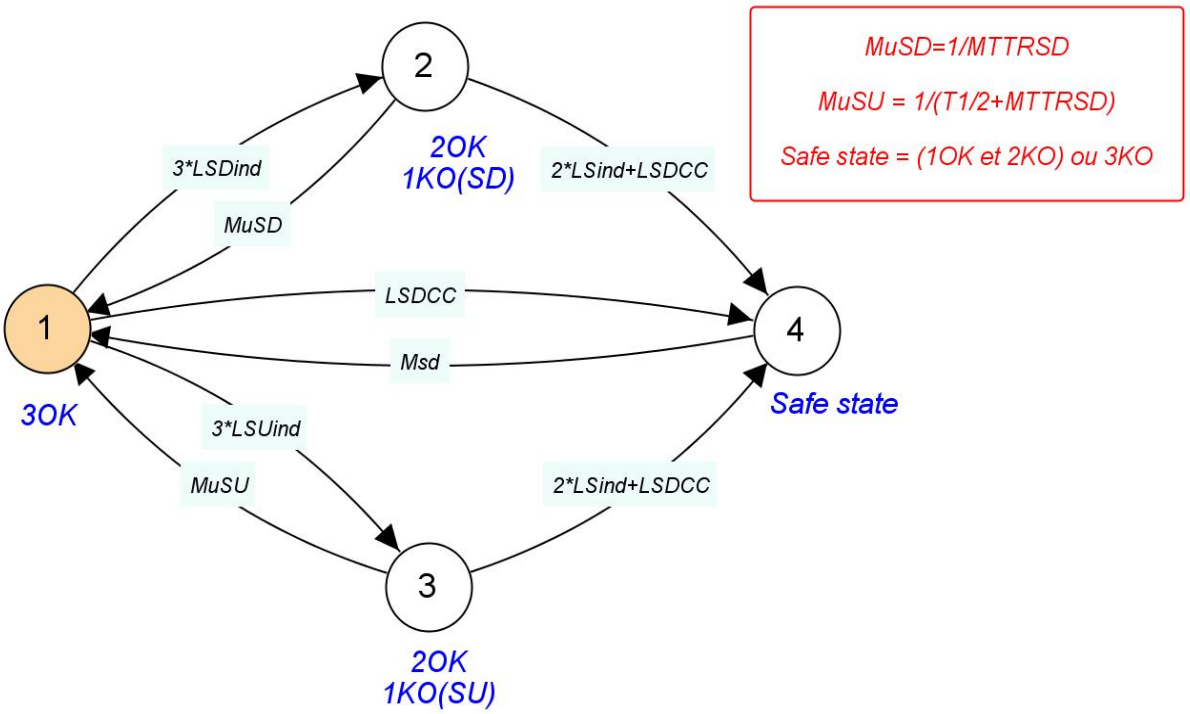

Figure 2.23 : Modélisation markovienne approchée des défaillances sûres de l'architecture 2*oo*3

Les probabilités asymptotiques issues du modèle de la figure 2.22 sont comme suit.

$$\left.\begin{aligned}
&P_1(\infty)=1-P_2(\infty)+P_3(\infty)+P_4(\infty)\approx 1\\
&P_2(\infty)=P_1(\infty).\frac{3\lambda_{SDind}}{\mu_{SD}+2\lambda_{Sind}+\lambda_{SDCC}}\approx\frac{3\lambda_{SDind}}{\mu_{SD}}=3\cdot(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}\\
&P_3(\infty)=P_1(\infty).\frac{3\lambda_{SUind}}{\mu_{SU}+2\lambda_{Sind}+\lambda_{SDCC}}\approx\frac{3\lambda_{SUind}}{\mu_{SU}}=3\cdot(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\\
&P_4(\infty)=P_1(\infty)\cdot\frac{\lambda_{SDCC}}{\mu_{sd}}+\left[P_2(\infty)+P_3(\infty)\right].\left[\frac{2\lambda_{Sind}+\lambda_{SDCC}}{\mu_{sd}}\right]\\
&\quad\approx 3\cdot\left[(2-\beta_{SD})\lambda_{SD}+(2-\beta_{SU})\lambda_{SU}\right]\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right]\cdot MTTR_{sd}\\
&\qquad+\lambda_{SDCC}\cdot MTTR_{sd}
\end{aligned}\right\} \quad (2.29)$$

On obtient alors :

$$PFS_{moy}^{2oo3}\approx 3\cdot\left[(2-\beta_{SD})\lambda_{SD}+(2-\beta_{SU})\lambda_{SU}\right]\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right]\cdot MTTR_{sd}+\lambda_{SDCC}\cdot MTTR_{sd} \quad (2.30)$$

$$STR_{2oo3} \approx 3\cdot\left[(2-\beta_{SD})\lambda_{SD}+(2-\beta_{SU})\lambda_{SU}\right]\cdot\left[(1-\beta_{SD})\cdot\lambda_{SD}\cdot MTTR_{SD}+(1-\beta_{SU})\cdot\lambda_{SU}\cdot\left[\frac{T_1}{2}+MTTR_{SD}\right]\right] + \lambda_{SDCC} \quad (2.31)$$

Le tableau 2.19 regroupe, toujours pour les mêmes données, les résultats numériques relatifs à l'architecture 2*oo*3.

Approches	*DC$_S$ %*	*PFS*	*STR (h^{-1})*
GRIF Multi-phases	***0***	3.100E-4	1.292E-5
	60	1.736E-4	7.233E-06
	90	9.070E-5	3.779E-06
GRIF Markov approché	***0***	2.929E-4	1.221E-5
	60	1.673E-4	6.969E-06
	90	8.927E-5	3.720E-06
Formules	***0***	3.740E-4	1.560E-5
	60	1.870E-4	7.770E-5
	90	9.110E-5	3.800E-6

Tableau 2.19 : Résultats numériques relatifs aux PFS/STR de l'architecture 2*oo*3

La figure 2.24rassemble les différentes courbes relatives aux *PFS* et *STR* de l'architecture 2*oo*3, le facteur *DC* est toujours pris égale à 0.6.

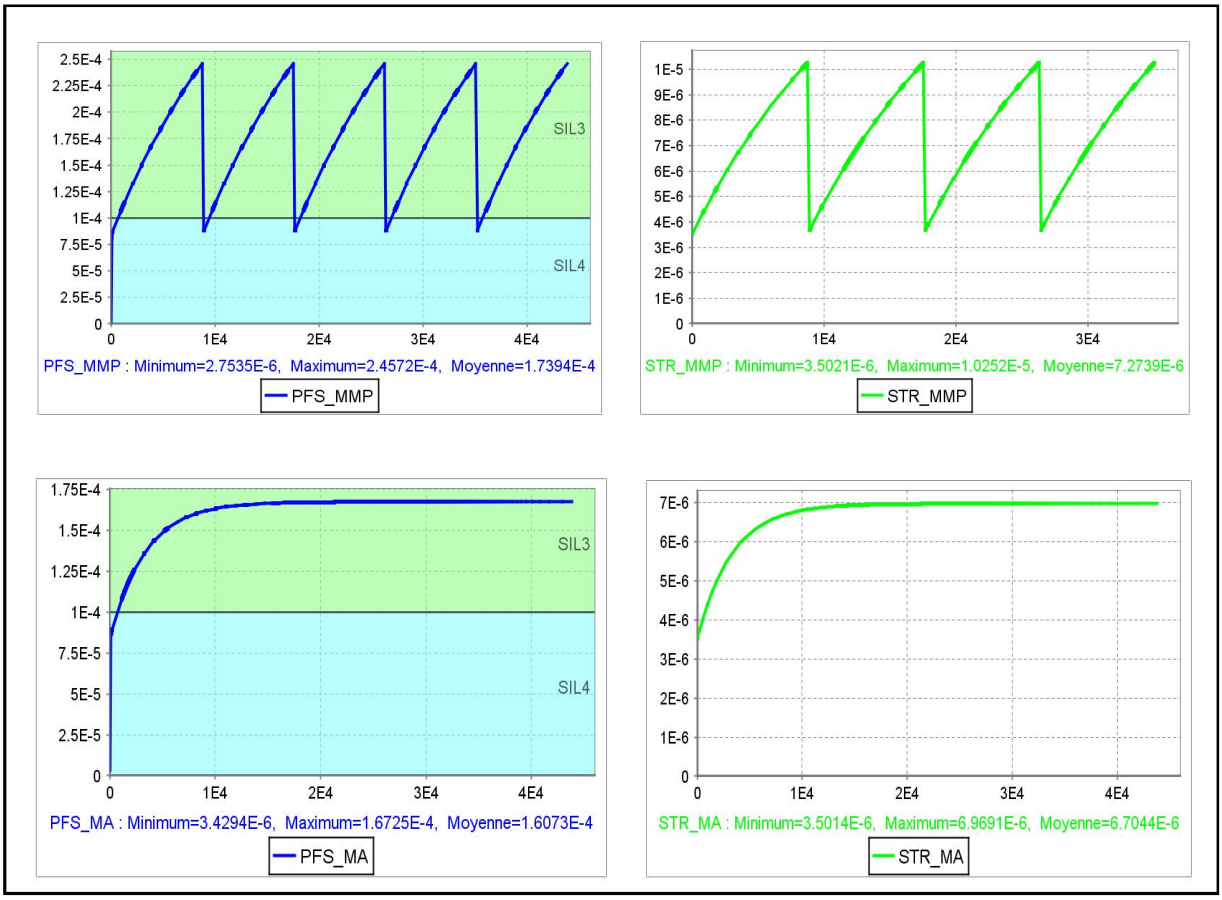

Figure 2.24 : Courbes relatives aux PFS/STR de l'architecture 2*oo*3

Les courbes fournies par les modèles markoviens approchés représentent une approximation de celles obtenues à partir des modèles multi-phases (sous-forme de dents de scie). Aussi, les valeurs moyennes obtenues via l'exploitation des courbes issues des modèles multi-phases sont approximées par les valeurs asymptotiques dégagées des courbes classiques. Cette approximation n'est valable qu'en régime stationnaire.

La lecture des tableaux 2.18 et 2.19 nous permet de constater que les résultats obtenus via une modélisation correcte (multi-phases) et une modélisation approchée sont voisins. Il convient de signaler que cette similitude n'est pas aussi forte que celle remarquée pour les architectures de type 1*ooN*. Aussi, les résultats qui découlent des modèles markoviens multi-phases sont systématiquement conservatifs par rapport à ceux issus d'une approche markovienne classique (approchée). Cependant, les formules analytiques fournissent les valeurs les plus pessimistes. Ceci est rassurant, par ce que sécuritaire, d'autant plus que l'usage des formulations analytiques est toujours favorisé par rapport aux modèles comportementaux, tels que les chaines de Markov.

2.5. Conclusion

Dans ce deuxième chapitre nous avons, dans un premier temps, regroupé les différentes formulations analytiques relatives aux performances des *SIS*, en termes d'intégrité opérationnelle et de sécurité. Nous avons, chaque fois l'information est disponible, souligner les différentes hypothèses selon lesquelles ces formulations ont été développées. Cela dit, l'ensemble des formules analytiques figurant au niveau de ce chapitre ne sont que des approximations et donc ne sont pas exactes. Il est alors évident que ces hypothèses restreignent l'usage de ces formules à l'étude d'architectures usuelles des *SIS* et qu'une approche holistique (*AdD*, chaînes de Markov, *RdP*, etc) est nécessaire pour des architectures non conventionnelles.

Un échantillon de résultats a ensuite été fourni à des fins de comparaison entre les différentes sources bibliographiques retenues dans le cadre de ce mémoire.

Nous avons finalement élaboré les formules analytiques relatives aux PFS_{moy} et *STR* des architectures *KooN* classiques. Pour ce faire, des modèles markoviens ont été développés et approchés (si nécessaire) afin d'extraire ces formules mathématiques. L'objectif de cette section était de vérifier la validité des différentes approches déjà existantes.

Les indicateurs de performances des *SIS* étant explicités en termes de formules mathématiques, le prochain chapitre est dévolu à l'optimisation des architectures des *SIS* compte tenu des différents objectifs établis (sécurité, disponibilité, maintenance, coûts, …).

CHAPITRE 3

Optimisation des architectures des SIS à l'aide des algorithmes génétiques (AG)

3.1. Introduction

Résoudre un problème d'optimisation consiste à rechercher, parmi un ensemble de solutions qui vérifient des contraintes données, la ou les solutions qui rendent minimale (ou maximale) une fonction mesurant la qualité de cette solution. Cette fonction est appelée *fonction objective*. Pour modéliser un problème d'optimisation, on commence en générale par définir les éléments qui composent les contraintes et la fonction objective. Parmi ces éléments, certains sont connus et sont appelés paramètres du problème et d'autres éléments sont inconnus et appelés inconnus ou *variables*. Les contraintes et la fonction objective s'expriment à l'aide de formules mathématiques qui combinent les paramètres connus et les variables du problème. Les variables correspondent souvent à des décisions à prendre de manière à obtenir l'optimum souhaité [PORTMAN, 2009].

Les méthodes directes d'optimisation (gradients, programmation dynamique, …) ne permettent pas de résoudre certains problèmes complexes qui ne possèdent pas de solution analytique exacte. Ces problèmes sont généralement caractérisés pars les faits suivants :

- Un espace de recherche vaste, où le problème possède énormément de paramètres devant être optimisés simultanément.
- Le problème ne peut être facilement décrit par un modèle mathématique précis : notamment lorsque la fonction à optimiser n'est pas continue.

A cet effet, un groupe de méthodes qualifiées d'heuristiques et méta-heuristiques, comprenant notamment le recuit simulé, la recherche taboue, les algorithmes génétiques, les colonies de fourmis, apparues a partir des années 1980, permettent de résoudre au mieux les problèmes dits d'optimisation difficile [SIARRY, 2009].

L'optimisation de l'architecture d'un *SIS* rentre dans cette catégorie d'optimisation difficile. Pour exposer les différentes facettes de même que la solution de cette optimisation, ce chapitre comporte deux parties complémentaires. Nous présentons d'abord le problème à optimiser au travers l'exemple d'un *HIPPS* (*High Integrity Pressure Protection System*). Cet exemple nous permet donc de mieux appréhender les différents aspects à prendre en compte dans le contexte des *SIS*. La méthode d'optimisation basée sur les algorithmes génétiques sera ensuite brièvement exposée et appliquée à cet exemple en mettant à profit l'outil «*Optimization Toolbox*» de l'environnement MATLAB [MATLAB, 2009].

Il convient de signaler que certains auteurs ont déjà exploité cette technique d'optimisation dans le cadre des *SIS* [SALLAK, 2007] [SALLAK *et al.*, 2008] [TORRES-ECHEVERRIA *et al.*, 2009]. Les travaux de Sallak portaient sur la minimisation de la PFD_{moy} d'un *SIS* sous la contrainte du coût de conception, sans prise en compte de l'intégrité opérationnelle du *SIS* (PFS_{moy}/STR). De plus, seuls les taux de défaillances détectées (λ_{DD}) et de réparation ($\mu_{DD}=1/MTTR_{DD}$) ont été pris en compte. Torres-Echeverría, quant à lui, a proposé une optimisation multi-objective intégrant les deux aspects : sécurité (PFD_{moy}) et disponibilité (STR). Néanmoins, les paramètres K et $T1$ n'étaient pas considérées comme variables (K=1 ; $T1$= 1an). Aussi, la méthode de quantification de l'indicateur *STR*, utilisée par Torres- Echeverría, nous semble fausse.

Nous précisons également que cette méthode d'optimisation n'est pas la seule applicable dans notre cas de figure.

3.2. Description du problème à optimiser

Introduisons dans un premier temps l'*HIPPS* présenté à la figure 3.1.

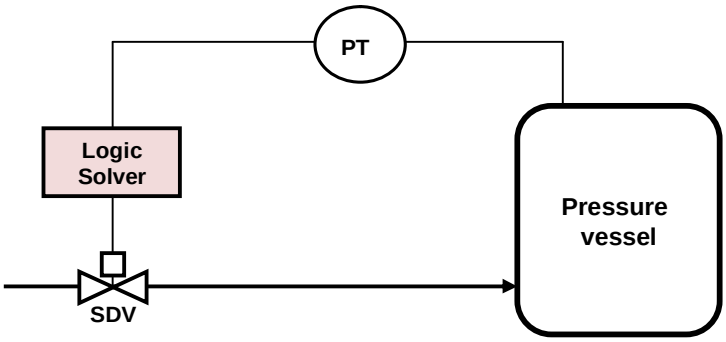

Figure 3.1: HIPPS à optimiser

Il s'agit d'un *SIS* protégeant un réservoir sous pression. En cas de surpression dans le réservoir (la pression dépasse un niveau-seuil donné), celle-ci est détectée par un ensemble de capteurs *PT* (*Pressure Transmitter*) qui transmettent l'information aux unités logiques *LS* (*Logic Solver*). Ces dernières commandent alors la fermeture des vannes de sécurité *SDV* (*Shutdown Valve*), ce qui a pour effet de faire baisser la pression dans le réservoir.

Le problème que l'on rencontre à ce stade est le choix des différents paramètres de conception relatif à ce système de protection, de telle sorte que les objectifs de sécurité et de production soient respectés. Dans notre cas ces objectifs sont formalisés comme suit :

- $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$. La PFD_{moy}^{MAX} est la valeur maximale autorisée pour la PFD_{moy} qui peut être déterminée à partir d'une analyse des risques de l'installation concernée (*SIL* requis). L'utilisation d'une méthode quantitative (de type *LOPA*) dans l'établissement du *SIL* requis permet d'obtenir directement la valeur de PFD_{moy}^{MAX} :

$$w_{acc} \approx w_{EI} \cdot \prod_i PFD_{moy}^{i} \cdot PFD_{moy}^{SIS} \leq w_t \tag{3.1}$$

$$\Rightarrow PFD_{moy}^{SIS} \leq \frac{w_t}{w_{EI} \cdot \prod_i PFD_{moy}^{i}} \Rightarrow PFD_{moy}^{Max} = \frac{w_t}{w_{EI} \cdot \prod_i PFD_{moy}^{i}} \tag{3.2}$$

où
w_{acc} : fréquence de l'accident,
w_{EI} : fréquence de son événement initiateur,
PFD^{i}_{moy}: probabilité moyenne de défaillance sur demande de la barrière *i*,
w_t : fréquence tolérable.

En revanche, si les données quantitatives disponibles ne permettent pas l'utilisation d'une méthode de type *LOPA*, l'usage des méthodes qualitatives telles que le graphe de risque conduisent directement à la valeur du *SIL* requis. Dans ce cas, le recours au tableau 1.1 (voir chapitre 1) permet d'attribuer la borne supérieure de l'intervalle correspondant à la PFD_{moy}^{MAX} . A titre illustratif, si le *SIL* requis identifié était *SIL* 2, la PFD_{moy}^{MAX} serait prise égale à 10^{-2}.

- $STR_{moy}^{HIPPS} \leq STR_{moy}^{Max}$: STR_{moy}^{Max}, valeur maximale autorisée pour le STR_{moy}, peut être définie, sur la base d'un consensus, suivant une analyse économique en tenant compte des coûts d'arrêts intempestifs et des redémarrages consécutifs du procédé, de la situation économique de l'entreprise en question, … On peut écrire à titre d'exemple : $STR_{moy}^{Max} \leq 1/an = 1.142E-4/h$. Bien entendu, plus les coûts induits par un arrêt intempestif sont importants, plus la valeur de STR_{moy}^{Max} est faible.

A ce titre, nous donnons ci-après une démarche développée par M.J.M. Houtermans [HOUTERMANS, 2006], dans le cadre de sa société, qui définit un indicateur breveté dénommé *STL* (*Spurious Trip Level*). Cet indicateur complète le *SIL* et fournit aux utilisateurs un moyen de définir le niveau désiré de la disponibilité de production imputable aux fonctions instrumentés de sécurité. Le *STL* est une mesure de la fréquence avec laquelle une fonction de sécurité est déclenchée en l'absence de toute demande émanant du procédé surveillé, qui sera donc mis à l'arrêt d'une manière intempestive

La démarche de M.J.M. Houtermans est largement inspirée de celle qui a produit la filiation entre les notions de risque tolérable, réduction de risque, de *SIL* et enfin de PFD_{moy}. On y trouve, dans le même ordre, les notions de coût liées aux pertes de production imputables aux déclenchements intempestifs, de réduction de ces déclenchements, de *STL* et enfin de PFS_{moy}.

Les relations entre ces quatre dernières entités apparaissent dans les deux tableaux suivants donnés dans [HOUTERMANS, 2006].

STL™	Description
6	Spurious trip costs over €20M
5	Spurious trip costs between €10M and €20M
4	Spurious trip costs between €5M and €10M
3	Spurious trip costs between €1M and €5M
2	Spurious trip costs between €500k and €1M
1	Spurious trip costs between €100k and €500k
None	Spurious trip costs between €0 and €100k

Tableau 3.1 : Relation entre coûts et STL

STL	Probability of fail safe (PFSavg)	Spurious Trip Reduction
X	$\geq 10^{-(X+1)}$ to $<10^{-X}$	$10^{X} - 10^{X+1}$
…	…	…
4	$\geq 10^{-5}$ to $<10^{-4}$	10000 – 100000
3	$\geq 10^{-4}$ to $<10^{-3}$	1000 – 10000
2	$\geq 10^{-3}$ to $<10^{-2}$	100 – 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	10 – 100

Tableau 3.2 : Relation entre STL et PFS_{moy}

Il convient de signaler que les formulations analytiques utilisées dans la suite de ce chapitre pour calculer les valeurs relatives aux deux objectifs précédents, PFD_{moy}^{HIPPS} et STR_{moy}^{HIPPS}, sont celles issues de l'approche binomiale, voir respectivement les formules 2.13 et 2.16. Elles peuvent en effet être utilisées d'une manière effective au niveau de la procédure d'optimisation présentée dans la suite de ce chapitre.

La réalisation des deux objectifs de disponibilité et de sécurité nécessite l'étude de plusieurs choix de conception et représente donc un problème d'optimisation qui peut se résumer ainsi :

1. Combien d'éléments au sein de chaque sous-système (*PT*, *LS*, *SDV*) sont nécessaires : 1, 2, …, *N*1/*N*2/*N*3 ? On fixe généralement un nombre maximal pour chacune de ces variables : $N1 \in [1, N1_{Max}]$; $N2 \in [1, N2_{Max}]$; $N3 \in [1, N3_{Max}]$.
2. Combien d'éléments au sein de chaque sous-système dont le fonctionnement est nécessaire : 1, 2, …, *K*1/*K*2/*K*3)? Bien entendu, les conditions suivantes doivent être satisfaites : $K1 \leq N1$; $K2 \leq N2$; $K3 \leq N3$.
3. Quel est le type des éléments de chacun des sous-systèmes : *PT*type {*PT*type$_1$, *PT*type$_2$, …, *PT*type$_i$}; *LS*type {*LS*type$_1$, LStype$_2$, …, *LS*type$_j$}; *SDV*type {*SDV*type$_1$, *SDV*type$_2$, …, *SDV*type$_k$}? Chaque type de composant possède ses propres paramètres fiabilistes : λ_D, λ_S, *DC*, DC_S, λ ,λ_D, λ_{SD}, λ_{SU}, $MTTR_{DD}$ (= $1/\mu_{DD}$), $MTTR_{SD}$ (= $1/\mu_{SD}$), C_A (coût d'acquisition), C_T (coût de tests périodiques).
4. Quel est l'intervalle de tests périodiques (*T*1) pour chaque sous-système : *PTT*1 {*PTT*1$_1$, *PTT*1$_2$, …, *PTT*1$_l$} ; *LST*1{*LST*1$_1$, *LST*1$_2$, …, *LST*1$_m$} ; *SDVT*1 {*SDVT*1$_1$, *SDVT*1$_2$, …, *SDVT*1$_n$} ?
5. Une contrainte supplémentaire sur le coût d'acquisition du *HIPPS*, en fonction du budget disponible, peut être établie : $C_A^{HIPPS} \leq C_A^{MAX}$. Avec :

$$C_A^{HIPPS} = N1 \cdot C_A^{PTtype} + N2 \cdot C_A^{LStype} + N3 \cdot C_A^{SDVtype} \tag{3.3}$$

Toujours dans le même ordre d'idées, les coûts de tests périodiques des différents constituants du *HIPPS* peuvent rentrer en ligne de compte. Cela dit, ce coût additionnel peut être calculé sur une durée de mission donnée (*TM*) à l'aide de la formule suivante :

$$C_T^{HIPPS} = N1 \cdot \frac{TM}{PTT1_l} \cdot C_T^{PTtype} + N2 \cdot \frac{TM}{LST1_m} \cdot C_T^{LStype} + N3 \cdot \frac{TM}{SDVT1_n} \cdot C_T^{SDVtype} \tag{3.4}$$

La contrainte précédente relative au coût devient alors : $\left.\begin{array}{l} C_A^{HIPPS} \leq C_A^{MAX} \\ C_T^{HIPPS} \leq C_T^{MAX} \end{array}\right\}$ (3.5)

La description du problème à optimiser permet de constater qu'une solution analytique exacte n'est pas envisageable. Le recours à une méthode d'optimisation numérique est donc indispensable. A cet effet, dans la suite de cette section, nous présentons brièvement les concepts de base des algorithmes génétiques (AG) de même que leur application pour l'optimisation du *HIPPS* précédent.

3.3. Principe et application des AG

3.3.1. Principe

Les algorithmes génétiques ont été développés à l'Université de Michigan par John Holland à la fin des années 60 [ELEGBEDE, 2003]. Ces algorithmes s'inspirent de l'observation de phénomènes biologiques, plus précisément de la capacité de populations d'organismes vivants à s'adapter à leur environnement à l'aide de mécanismes de sélection et d'héritage génétique [LUTTON, 2009]. Elles sont considérées comme une méthode numérique de recherche ayant pour objet l'optimisation d'un comportement donné, représenté sous forme d'une fonction dite « *fonction objective* » $f(x_i)$ d'un ou de plusieurs variables (x_i) éventuellement soumises à certaines contraintes $g(x_i)$ (linéaires ou non) [MARSEGUERRA *et al.*, 2006]. Le schéma général du déroulement d'un algorithme génétique est représenté à la figure 3.2.

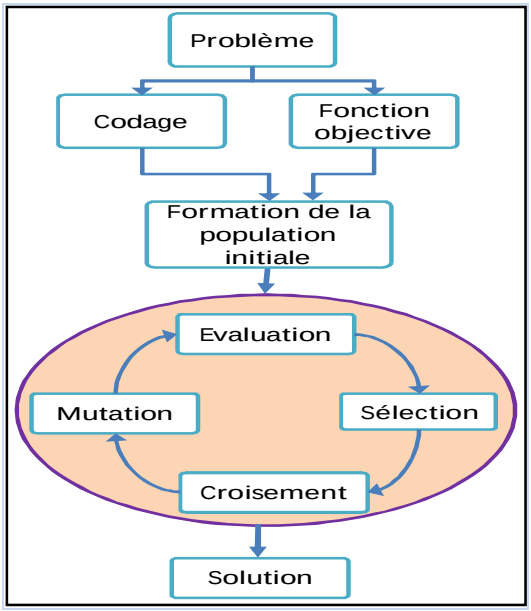

Figure 3.2 : Structure générale d'un AG

La recherche d'une solution à un problème d'optimisation à l'aide des *AG* requiert la présentation, avant toute chose, sous une *forme codée* de l'expression des solutions : *les chromosomes*. Dans notre cas, chaque configuration du *HIPPS* peut être codée par un chromosome de 12 *gènes* :

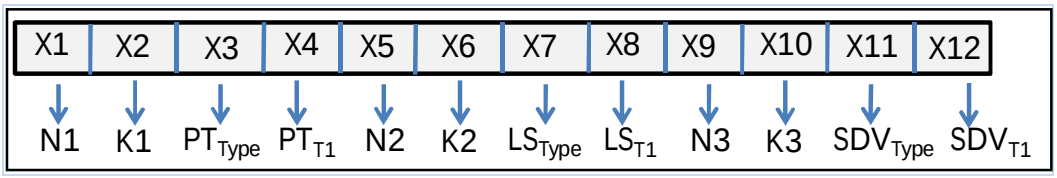

Figure 3.3 : Codage du HIPPS

Une fois le codage établi, il s'agit ensuite de générer aléatoirement, sur tout l'espace des solutions, une *population initiale* constituée d'individus (chaque individu est caractérisé par un chromosome), dont le nombre est fixé par l'utilisateur. L'AG consiste à faire évoluer progressivement, par *générations successives*, la composition de cette population en maintenant sa taille constante. D'une génération à la suivante, l'adaptation de la population, telle que représentée par la fonction objective, doit globalement s'améliorer. La génération d'une nouvelle population à partir de la précédente se fait en deux étapes : la *sélection* et la *reproduction*. Au

cours de la première étape, l'algorithme sélectionne les individus les mieux adaptés à ce reproduire (parents) et donner des descendants (enfants). Pour ce faire, il est nécessaire d'évaluer la performance de chaque individu selon la fonction objective. La sélection est une procédure stochastique qui respecte en général le principe suivant : plus un individu est compétent, plus sa probabilité de sélection est élevée. A ce titre, plusieurs méthodes ont été élaborées :

- ***Sélection par rang.*** Cette technique de sélection choisit toujours les individus possèdent les meilleurs scores d'adaptation, le hasard n'entre donc pas dans ce mode de sélection. En fait, si *n* individus constituent la population, la sélection appliquée consiste à conserver les *k* meilleurs individus (au sens de la fitness) suivant une probabilité qui dépend du rang (et pas de fitness).
- ***Sélection par roulette (Wheel).*** Pour chaque individu, la probabilité d'être sélectionné est proportionnelle à son adaptation au problème. Afin de sélectionner un individu, on utilise le principe de la roue de la fortune où chaque individu est représenté par une portion proportionnelle à son adaptation. La sélection s'effectue ensuite selon un tirage au sort homogène sur cette roue (voir figure 3.4).

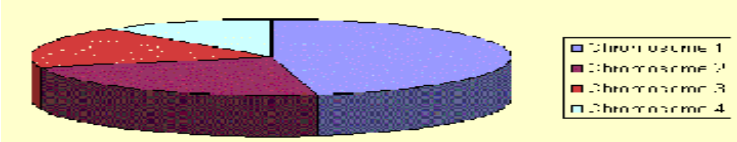

Figure 3.4 : Exemple de sélection par roulette

- ***Sélection par tournoi.*** Cette technique utilise la sélection proportionnelle sur des paires d'individus, puis choisit parmi ces paires l'individu qui a le meilleur score d'adaptation.
- ***Sélection uniforme.*** Cette sélection se fait aléatoirement, uniformément et sans intervention de la valeur d'adaptation. Chaque individu à donc une probabilité 1/*p* d'être sélectionné, ou *p* est le nombre total d'individu dans la population.
- ***Sélection steady–state.*** Ce n'est pas une méthode particulière de sélection des chromosomes parents. L'idée principale est qu'une grande partie de la population puisse survivre à la prochaine génération. L'*AG* marche alors de la manière suivante : à chaque génération sont sélectionnés quelques chromosomes (parmi ceux qui ont la meilleure adaptation) pour créer des chromosomes fils. Ensuite, les chromosomes les plus mauvais sont retirés et remplacées par les nouveaux, le reste de la population survie à la nouvelle génération.
- ***Elitisme.*** A la création d'une nouvelle population, il ya de grandes chances que les meilleures chromosomes soient perdus après les opérations de croisement et de mutation. Pour éviter cela, on utilise le principe d'élitisme qui consiste à copier un ou plusieurs des meilleurs chromosomes dans la nouvelle génération. Ensuite, on génère le reste de la population selon l'algorithme de reproduction usuel. Cette méthode améliore considérablement les *AG*, car elle permet de ne pas perdre les meilleures solutions.

Les individus issus du mécanisme de sélection sont ensuite soumis à la reproduction à l'aide de deux procédures stochastiques : croisement et mutation. Le croisement est basé sur un principe d'échange des propriétés entre deux individus et implique la naissance de deux nouveaux individus. Un croisement débute par une sélection aléatoire des couples d'individus à croiser. Les points de croisement peuvent également être choisis aléatoirement. Généralement, le croisement est effectué selon une probabilité *Pc* (pour *Pc* = 0.6, le croisement n'est effectué que si *R* (nombre aléatoire) < 0.6).

La mutation consiste en une variation aléatoire de n'importe quel gène du chromosome appartenant aux solutions issues de la phase de sélection et ayant subies ou non une procédure de croisement. Rien ne nous dit que l'individu muté sera meilleur ou moins bon, mais il apportera des possibilités supplémentaires qui pourraient bien être utiles pour la création de bonnes solutions. Comme pour le croisement, la mutation s'effectue sur un individu donné selon une probabilité *Pm* usuellement très faible (par exemple, *Pm* = 0.02). Un exemple de croisement et de mutation est présenté à la figure 3.5.

La constitution de la génération n+1 s'effectue par *remplacement*. A cet effet, plusieurs méthodes ont été élaborées. On peut, par exemple, remplacer les plus « mauvais » individus (au sens de la fonction objective) de la population courante par les meilleurs individus produits (en nombre égal). L'algorithme est interrompu après la satisfaction d'un critère d'arrêt : nombre maximal de générations, par exemple.

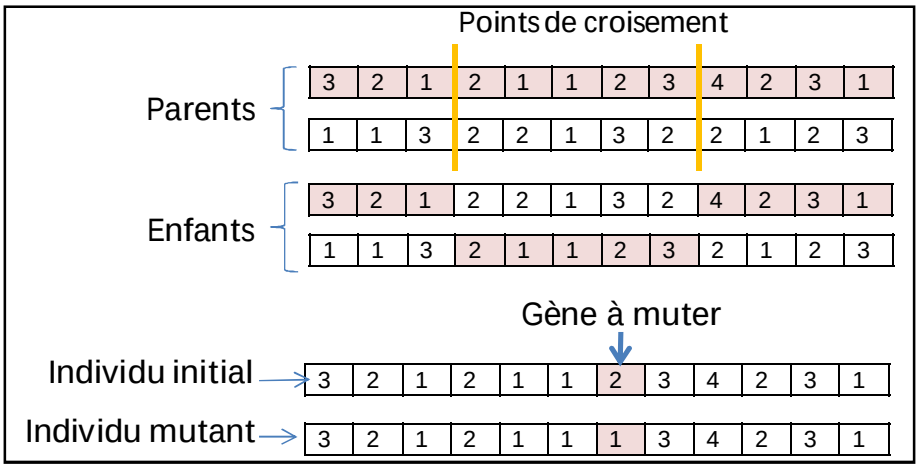

Figure 3.5 : Exemple d'opérateurs de croisement et de mutation

Reste à appliquer cette démarche à notre exemple illustratif. C'est l'objet de la section suivante.

3.3.2. Optimisation de l'architecture du HIPPS

Les données nécessaires à l'optimisation du *HIPPS* sont groupées au tableau 3.3. De plus, l'allocation des barrières de sécurité, réalisée d'une manière qualitative, a établi un *SIL requis* = 3. Ceci revient à écrire la contrainte liée à la PFD_{moy} comme suit : $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX} = 1E-3$.

Aussi, $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX} = 0.5/an = 5.71E-5/h$. Si l'on considère une *MTTRsd* = 84 *h* (une semaine), cette objectif en termes de *STR* pourrait correspondre à un *STL 2* (voir relation 2.20 et tableau 3.2).

Dans ce qui suit, nous allons tester plusieurs stratégies d'optimisations qui sont listées ci-après.

1. Minimisation de la PFD_{moy}^{HIPPS} sans aucunes contraintes.
2. Minimisation de la PFD_{moy}^{HIPPS} sous les contraintes : $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$ et $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX}$.

3. Minimisation de la PFD_{moy}^{HIPPS} sous les contraintes : $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$, $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX}$ et $C_A^{HIPPS} \leq C_A^{MAX}$.
4. Minimisation de la PFD_{moy}^{HIPPS} sous les contraintes : $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$, $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX}$, $C_A^{HIPPS} \leq C_A^{MAX}$ et $C_T^{HIPPS} \leq C_T^{MAX}$.
5. Optimisation multi-objectifs (minimisation parallèle d'un ensemble d'objectifs) : PFD_{moy}^{HIPPS}, STR_{moy}^{HIPPS}, C_A^{HIPPS} et C_T^{HIPPS}.

Données	Types des composants : **λ** (10^{-6}/h) ; MTT R (h) ; C_A (unités) ; C_T (unités) ; **λ** = **λ** $_{SU}$ = **2λ** $_D$=2 **λ** $_{SD}$			T1(h)
Sous-systèmes	Type 1	Type 2	Type 3	
PT $N1_{Max}$= 5	λ_D =0.151 DC = 0.318 λ_S =0.383 DCS = 0.692 β = 0.02 λ = 0.02 $MTTR_{DD}$= 4 $MTTR_{SD}$= 8 C_A = 4844 C_T = 4844	λ_D =1.9 DC = 0.51 λ_S =2.16 DCS = 0.56 β = 0.02 λ = 0.02 $MTTR_{DD}$= 8 $MTTR_{SD}$= 10 C_A = 2306 C_T = 4844	λ_D = 4.11 DC = 0.1 λ_S = 6.81 DCS = 0.1 β = 0.05 λ = 0.05 $MTTR_{DD}$= 10 $MTTR_{SD}$= 10 C_A = 500 C_T = 4844	4380 8760 13140 17520
LS $N2_{Max}$= 3	λ_D = 0.01 DC =0.9 λ_S =0.01 DCS =0.2 β = 0.01 λ = 0.01 $MTTR_{DD}$= 4 $MTTR_{SD}$= 4 C_A = 4000 C_T = 4844	λ_D =10 ; DC =0.9 λ_S =10 ; DCS =0.2 β = 0.01 λ = 0.01 $MTTR_{DD}$= 8 $MTTR_{SD}$= 8 C_A = 2800 C_T = 4844	λ_D =15 DC =0.67 λ_S = 15 DCS = 0.2 β = 0.01 λ = 0.01 $MTTR_{DD}$= 8 $MTTR_{SD}$= 10 C_A = 2000 C_T = 4844	8760 13140 17520
SDV $N3_{Max}$= 4	λ_D = 3.35 DC = 0.25 λ_S = 3.94 DCS = 0 β = 0.02 λ = 0.02 $MTTR_{DD}$= 8 $MTTR_{SD}$ =8 C_A = 6940 C_T = 4844	λ_D = 5.44 DC = 0.20 λ_S=3.17 DCS = 0 β = 0.05 λ = 0.05 $MTTR_{DD}$= 8 $MTTR_{SD}$=10 C_A = 6500 C_T = 4844	λ_D = 7.9 DC = 0.1 λ_S = 9.17 DCS = 0 β = 0.1 λ = 0.1 $MTTR_{DD}$=10 $MTTR_{SD}$=15 C_A = 6000 C_T = 4844	2190 4380 8760 13140 17520

Tableau 3.3 : Paramètres relatifs au HIPPS à optimiser

Afin de faciliter l'usage des algorithmes génétiques, leur déroulement est désormais entièrement supporté par l'outil «*Optimization Toolbox*» de l'environnement MATLAB, dont l'interface est représenté à la figure 3.6. Sa description est donnée dans la suite de ce chapitre en fonction, au fur et à mesure, des différentes stratégies d'optimisation définies précédemment.

Pour accéder à cet outil, il suffit d'écrire *optimtool* dans la fenêtre de commande de MATLAB. On peut également utiliser la fenêtre principale de MATLAB comme le montre la figure 3.7.

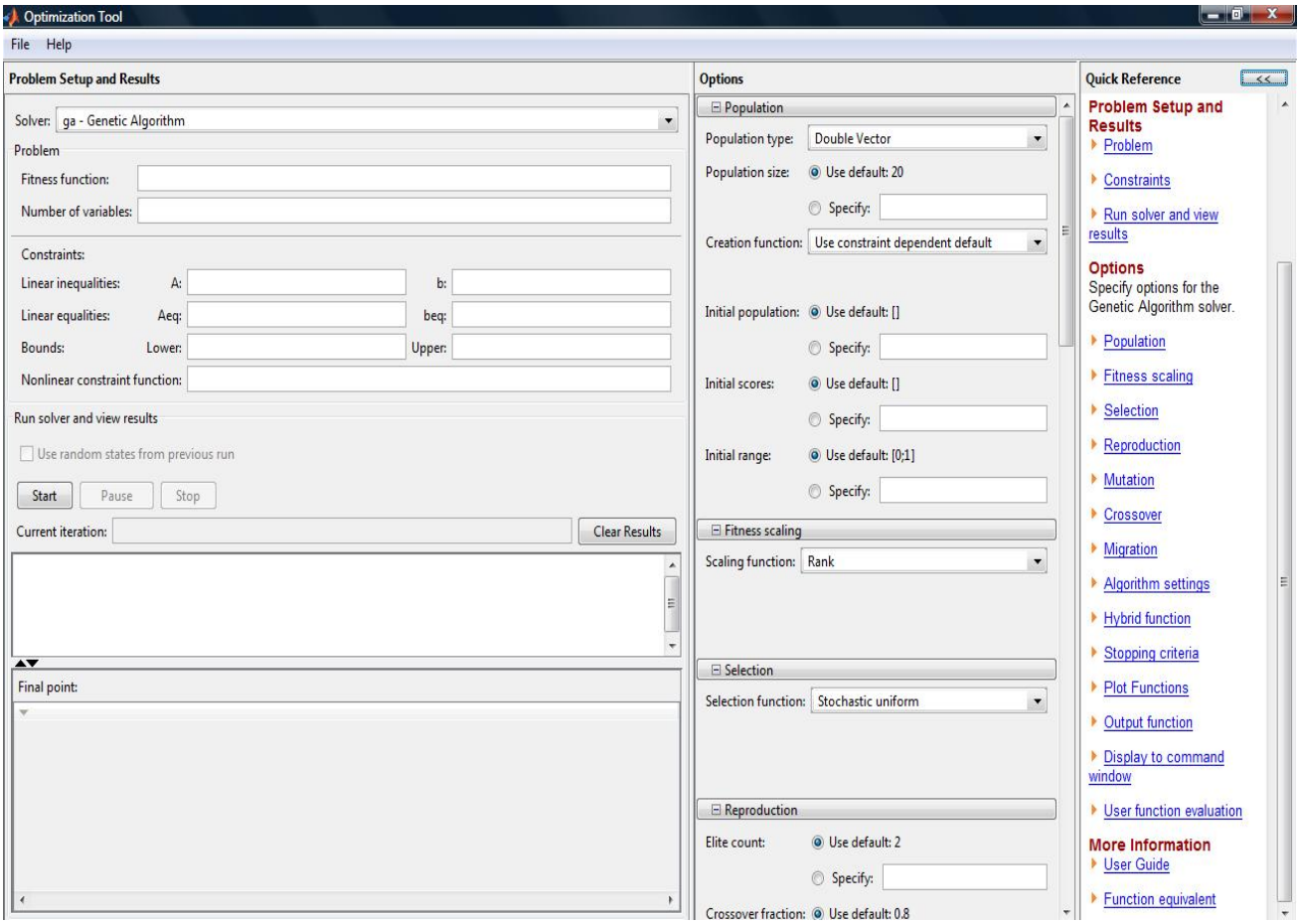

Figure 3.6 : Interface graphique de l'outil Optimization Toolbox

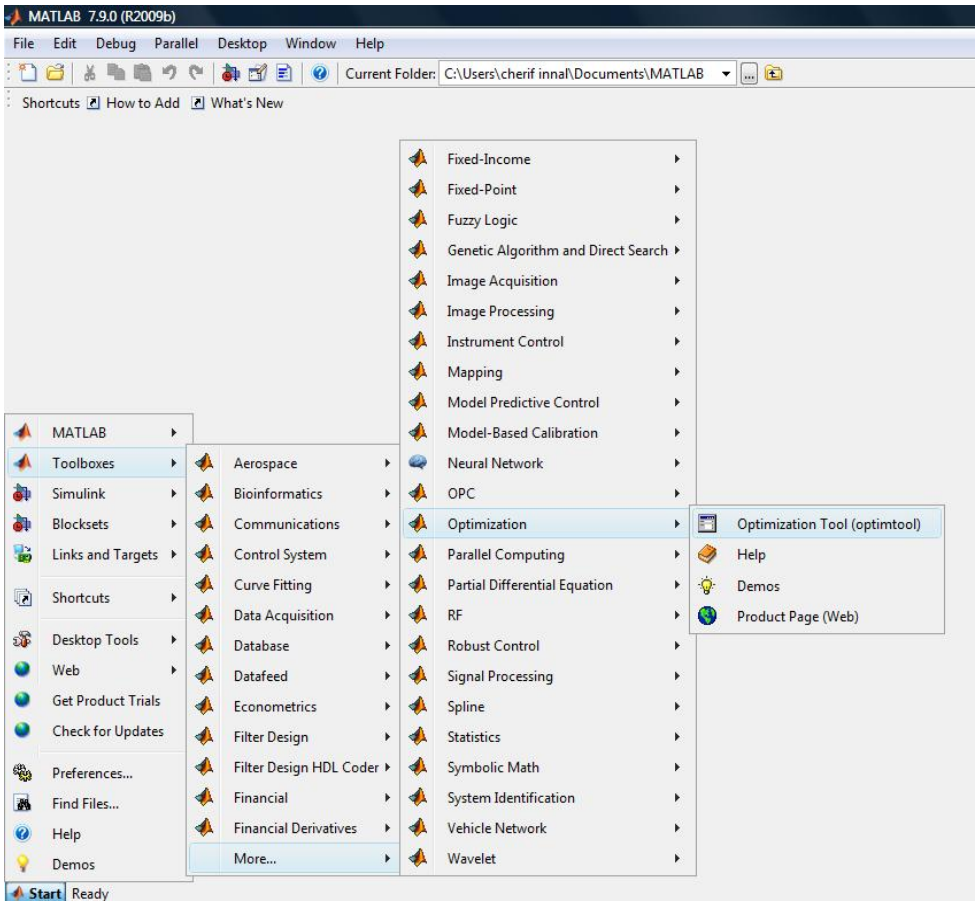

Figure 3.7: Obtention de l'interface graphique de l'outil Optimization Toolbox

Comme nous l'avons déjà signalé, rappelons-le, de différentes stratégies d'optimisation seront explorées. Voyons cela.

3.3.2.1. *Stratégie* 1 : *minimisation de la* PFD_{moy}^{HIPPS} *sans aucunes contraintes.* Ce type d'optimisation est communément appelé *SOP* (*single-objective optimization problem*), où une *seule fonction* objective est considérée : PFD_{moy}^{HIPPS} dans notre cas. Il importe de signaler que des contraintes peuvent être incluses (stratégies 2, 3 et 4). Aussi, une seule solution (solution optimale) est retournée par le Solveur.

Afin de réaliser une telle optimisation, au niveau de l'outil *Optimization Toolbox*, l'utilisateur doit suivre les étapes suivantes (voir figure ci-après) :

- Choisir le Solveur convenable à partir du champ ***Solver*** : *ga-Genetic Algorithm.*
- Faire appel de la *fonction objective à minimiser* (PFD_{moy}^{HIPPS}) dans le champ ***Fitness function.*** Elle doit être saisie sous la forme suivante : @nom de la fonction (dans notre cas : @SIS_OPT). SIS_OPT est donnée par l'équation (2.9 et 2.13) et écrite dans un fichier «*M-File*» (voir annexe 1).
- Introduire le nombre de variables dans le champ ***Number of variables*** : 12 variables.
- Définir les intervalles de recherche correspondants dans le champ ***Contsraints*** (contraintes linéaires). Trois types d'informations peuvent être renseignés :

- *Inégalités linéaires :* elles sont de la forme $A.x \leq b$, A est une matrice et b est un vecteur. Pour le problème d'optimisation considéré, ces inégalités s'écrivent comme suit.

$$\left.\begin{array}{l} -N1+K1 \leq 0 \Leftrightarrow -X1+X2 \leq 0 \\ -N2+K2 \leq 0 \Leftrightarrow -X5+X6 \leq 0 \\ -N3+K3 \leq 0 \Leftrightarrow -X9+X10 \leq 0 \end{array}\right\}$$

Cette écriture est saisie au niveau de l'interface graphique sous la forme suivante :

$$\begin{bmatrix} -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} X1 \\ X2 \\ X3 \\ X4 \\ X5 \\ X6 \\ X8 \\ X9 \\ X10 \\ X11 \\ X12 \\ X13 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

- *Egalités linéaires :* elles sont de la forme *Aeq.x = beq*, Aeq est une matrice et beq est un vecteur. Ce type de contraintes n'existe pas pour l'optimisation considérée.
- *Bornes inférieures* (***Lower***) et *supérieures* (***Upper***) de l'ensemble des variables (voir tableau 4.3). Ces bornes sont définies respectivement, au niveau de l'interface graphique, par les deux vecteurs suivants : [1 1 1 1 1 1 1 1 1 1 1] et [5 5 3 4 3 3 3 3 4 4 3 5].

- Sélectionner les options de l'algorithme : nombre des individus dans la population (200), type de sélection (Tournament : tournoi), type de croisement (Two point : deux points) et de mutation (Adaptive feasible), critère d'arrêt (nombre maximal de génération, …). On peut également au niveau du menu option demander certains types de graphiques tels que : Best fitness (valeur minimale de la fonction objective), Best individual (composition du vecteur des variables répondant à cette valeur minimale), …
- Lancer l'exécution en appuyant sur le bouton ***Start***. Les résultats s'affichent, une fois le critère d'arrêt atteint, dans le champ ***Final point* :** le vecteur des variables retourné par le logiciel correspond à la solution optimale.

Pour cette première stratégie d'optimisation ce vecteur est : **[5 1 1 1 3 1 1 1 4 1 1 1]**. Ce résultat est tout à fait logique et complètement prévisible. Ce constat montre la validité de notre approche d'optimisation.

Le résultat obtenu satisfait à l'architecture suivante : 1oo5 (PT de type1, testés chaque 6 mois) ; 1oo3 (LS de type1, testées chaque an) ; 1oo4 (SDV de type1, testées chaque 3 mois). La valeur de PFD_{moy}^{HIPPS} qui en découle est 6.0058E-5.

L'évolution de la fonction objective en fonction des générations est donnée à la figure 3.8. On remarque qu'elle atteint une valeur stationnaire à partir de la 9ème génération.

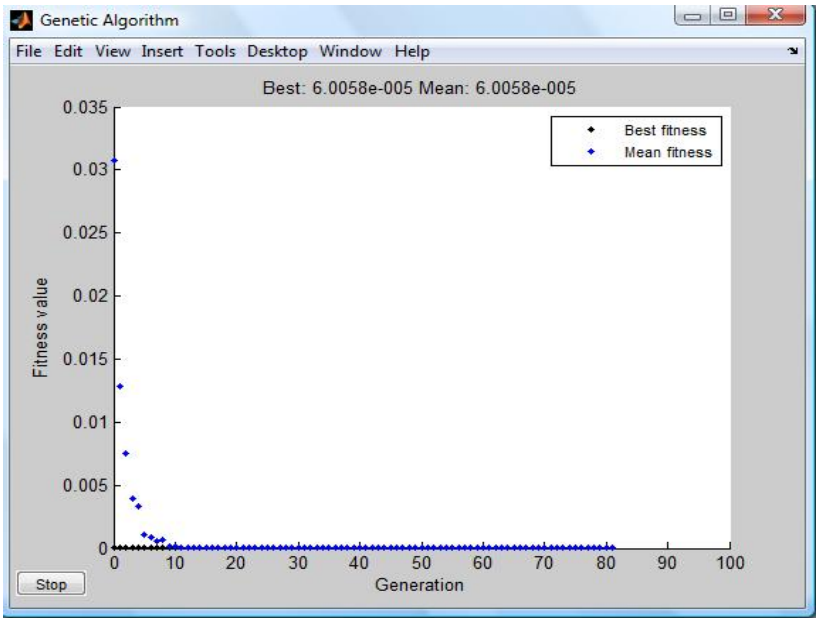

Figure 3.8 : Fonction objective en fonction des générations (stratégie 1)

3.3.2.2. *Stratégie 2 : minimisation de la PFD_{moy}^{HIPPS} sous les contraintes $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX} = 1E-3$ et $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX} = 5.71E-5/h.$* Pour cette deuxième stratégie d'optimisation, le paramétrage de l'interface graphique est identique au précédent excepté l'ajout des contraintes non linéaires dans le champ ***Nonlinear constraint function***. Comme pour la fonction objective, la fonction des contraintes doit être saisie sous la forme suivante : @nom de la fonction des contraintes (dans notre cas : @SIS_OPT_CONST). Cette dernière est écrite dans un fichier «*M-File*».

Le résultat trouvé (au terme de 19 générations, voir figure 3.9) est le même que précédemment, c'est-à-dire : **[5 1 1 1 3 1 1 1 4 1 1 1]**. Le STR_{moy}^{HIPPS} relatif à ce vecteur de variables est égal à 1.7448E-5/*h*. Cette valeur est donc inférieure à $STR_{moy}^{MAX} = 5.71E-5/h.$

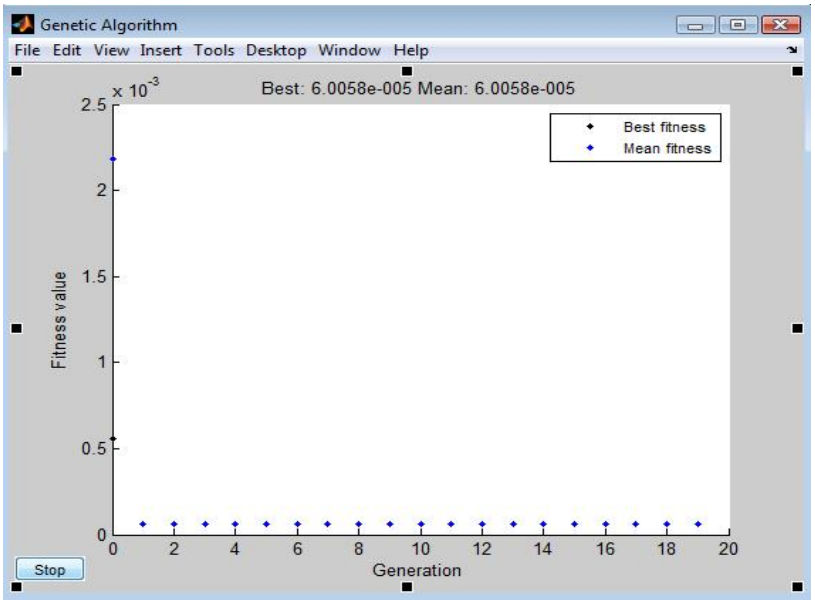

Figure 3.9: Fonction objective en fonction des générations (stratégie 2)

3.3.2.3. Stratégie 3 : minimisation de la PFD_{moy}^{HIPPS} ***sous les contraintes*** $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$**,** $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX}$ ***et*** $C_A^{HIPPS} \leq C_A^{MAX}$. Cette fois-ci, en gardant les mêmes contraintes précédentes, nous les augmentons par l'addition d'une contrainte supplémentaire liée au coût d'acquisition du *HIPPS* : $C_A^{HIPPS} \leq C_A^{MAX} = 32000$ unités.

La solution optimale retournée par le logiciel est : **[2 1 1 1 2 1 1 1 2 1 1 1]**. Les valeurs de PFD_{moy}^{HIPPS} et STR_{moy}^{HIPPS} sont respectivement 7.01E-5 (voir figure 3.10) et 8.582E-6/h. Le coût global d'acquisition s'élève à 31568 unités. On peut donc constater que l'ensemble des objectifs est respectés.

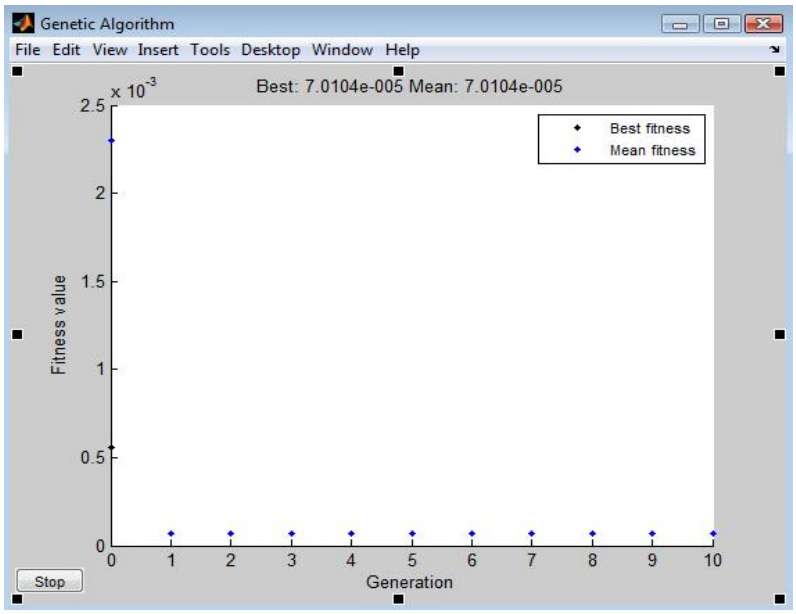

Figure 3.10: Fonction objective en fonction des générations (stratégie 3)

3.3.2.4. *Stratégie 4* : *minimisation de la* PFD_{moy}^{HIPPS} ***sous les contraintes :*** $PFD_{moy}^{HIPPS} \leq PFD_{moy}^{MAX}$**,** $STR_{moy}^{HIPPS} \leq STR_{moy}^{MAX}$ **,** $C_A^{HIPPS} \leq C_A^{MAX}$ ***et*** $C_T^{HIPPS} \leq C_T^{MAX}$**.** Cette quatrième stratégie comporte une deuxième contrainte sur le coût des tests périodiques (sur une période d'observation *TM* = 30 ans) des différents constituants du *HIPPS* : $C_T^{HIPPS} \leq C_T^{MAX} = 18000$ unités.

Le vecteur **[2 1 1 3 2 1 1 2 2 1 1 1]** est le résultat de l'optimisation correspondant à la stratégie 4. Les valeurs de PFD_{moy}^{HIPPS} et STR_{moy}^{HIPPS} sont respectivement 7.9673E-5 (figure 3.11) et 8.582E-6/h. Le coût global d'acquisition s'élève à 31568 unités, tandis que celui relatif aux tests périodiques vaut 17867 unités. Encore, une fois de plus, les objectifs établis sont tous satisfaits.

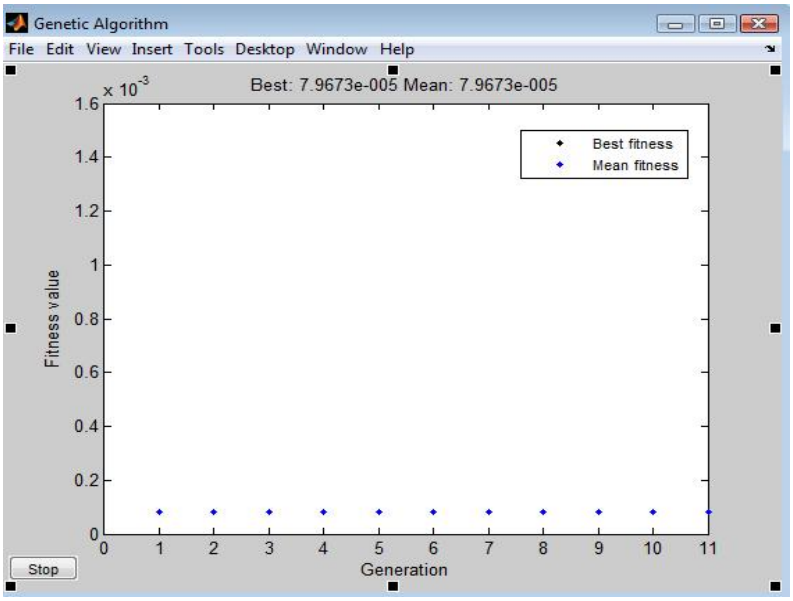

Figure 3.11: Fonction objective en fonction des générations (stratégie 4)

3.3.2.5. *Stratégie 5* : optimisation multi-objectifs (minimisation parallèle d'un ensemble d'objectifs) : PFD_{moy}^{HIPPS}, STR_{moy}^{HIPPS}, C_A^{HIPPS} et C_T^{HIPPS}.

Dans ce cas, la minimisation de PFD_{moy}^{HIPPS} n'est plus prioritaire par rapport au respect des différentes contraintes qui s'y associent. Comme son non l'indique, une optimisation multi-objectifs consiste en une minimisation simultanée de différents objectifs, qui sont donc sur les mêmes pieds d'égalité vis-à-vis de l'optimisation. Ca va de soi, l'algorithme ne retourne pas une seule solution, mais plusieurs solutions et qui sont toutes optimales par rapport l'un ou l'autre des objectifs : solutions non dominantes (***Pareto front*** (voir figure 3.12)).

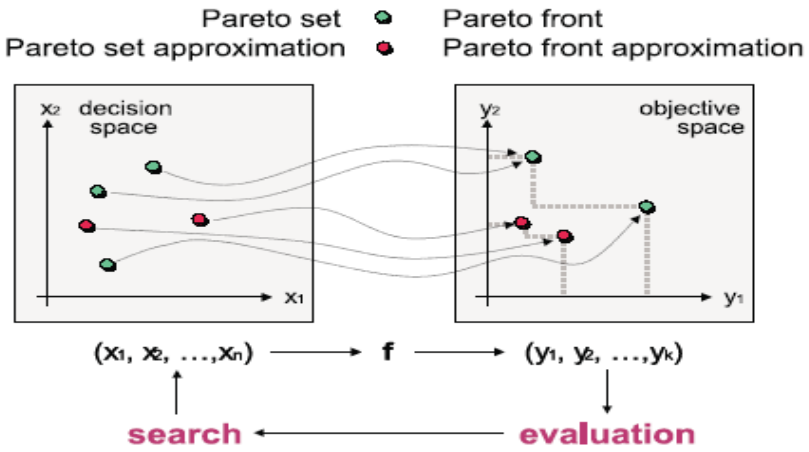

Figure 3.12: Cadre général d'une optimisation multi-objectifs [ECKART ZITZLER et al., 2002]

Pour effectuer ce type d'optimisation, au niveau de l'interface graphique, il est nécessaire de :

- Sélectionner le Solver convenable : ***gamultiobj-Multiobjective optimization using Genetic Algorithm***.

- Faire appel de la *fonction objective*, qui contient cette fois-ci plusieurs objectifs à minimiser, dans le champ ***Fitness function :*** @ SIS_Multiobj_OPT (écrite dans un fichier «*M-File*»).

Après avoir exécuté l'algorithme, les meilleures solutions trouvées sont données au tableau 3.4, tandis que les valeurs respectives relatives ou quatre objectifs sont données au tableau 3.5. La figure 3.13 montre le *Front de Pareto* relatif aux objectifs de sécurité (PFD_{moy}) et de disponibilité (*STR*).

5	1	1	1	3	1	1	1	4	1	1	1
1	1	3	3	1	1	3	2	1	1	3	3
1	1	3	4	1	1	3	3	1	1	3	5
5	5	1	1	3	3	1	1	4	4	1	1
3	3	3	4	3	3	3	3	4	4	3	5
5	1	3	1	2	2	1	1	2	1	1	1
5	4	1	1	3	1	1	1	3	2	2	1
5	1	1	1	2	1	1	1	4	1	1	1
4	4	3	4	3	3	3	3	4	3	3	2
3	2	1	1	1	1	1	1	4	2	1	2
4	2	2	1	3	2	1	3	2	2	2	1
5	2	1	4	3	3	2	1	2	2	3	1
3	3	3	4	3	2	1	3	4	4	3	5
4	4	1	1	1	1	1	1	4	4	1	1
1	1	3	1	1	1	1	1	2	1	2	2
3	3	3	4	2	2	2	2	2	2	3	5
3	3	1	4	2	2	3	2	3	3	3	5
2	1	3	1	2	1	3	3	1	1	3	5
3	3	3	3	3	3	3	3	4	4	3	4
2	1	3	3	1	1	3	2	1	1	3	1
3	3	3	3	2	1	1	1	3	1	1	5
2	1	1	1	1	1	1	1	4	1	1	1
3	3	1	1	3	3	1	1	4	3	1	2
3	3	3	1	3	3	3	3	4	4	3	5
3	1	3	1	3	1	3	1	4	1	3	5
3	1	1	1	3	1	1	1	2	2	1	1
1	1	3	4	1	1	3	3	2	2	3	5
5	1	1	1	3	2	1	1	2	1	1	1
4	2	1	1	1	1	1	1	4	2	1	2
5	1	1	1	3	1	1	1	4	1	1	1
5	1	1	1	2	1	1	1	4	1	1	1
3	3	3	4	3	3	3	3	4	4	3	5
5	4	1	1	3	1	1	1	3	2	2	1
5	1	1	1	3	2	1	1	3	1	1	1

Tableau 3.4 : Front de Pareto (solutions non dominantes)

PFD_{moy}	STR	C_A	C_T
6,01E-05	1,74E-05	63980	45000
0,08853124	3,10E-05	8500	2000
0,13882663	3,10E-05	8500	1200
0,01210239	8,39E-08	63980	45000
0,45633324	2,12E-06	31500	4200
0,0004813	4,06E-05	24380	21200
0,0003302	2,53E-07	55720	33000
6,01E-05	1,74E-05	59980	43600
0,25842141	2,07E-06	32000	11600
0,00012097	4,88E-07	46292	23000
0,0094665	2,63E-07	34224	18100
0,02838941	1,22E-06	44620	15600
0,32632038	1,33E-06	37500	5100
0,01187127	9,38E-08	51136	39800
0,00875683	1,30E-05	17500	7800
0,22673698	3,63E-06	19100	3133,33333
0,24340589	3,56E-06	36532	4666,66667
0,06608675	5,23E-05	11000	3000
0,37485639	2,07E-06	31500	5200
0,04258837	3,75E-05	9000	5866,66667
0,07123975	1,20E-05	30320	6300
6,45E-05	1,63E-05	41448	35000
0,00103192	8,84E-08	54292	25800
0,38567393	2,05E-06	31500	6000
0,00691448	9,84E-05	31500	7200
0,0055188	1,28E-06	40412	25800
0,19526478	2,39E-05	14500	1800
7,00E-05	9,70E-06	50100	30600
0,00012077	4,88E-07	51136	25400
6,01E-05	1,74E-05	63980	45000
6,01E-05	1,74E-05	59980	43600
0,45633324	2,12E-06	31500	4200
0,0003302	2,53E-07	55720	33000
6,01E-05	1,36E-05	57040	37800

Tableau 3.5 : Valeurs relatives aux objectifs établis

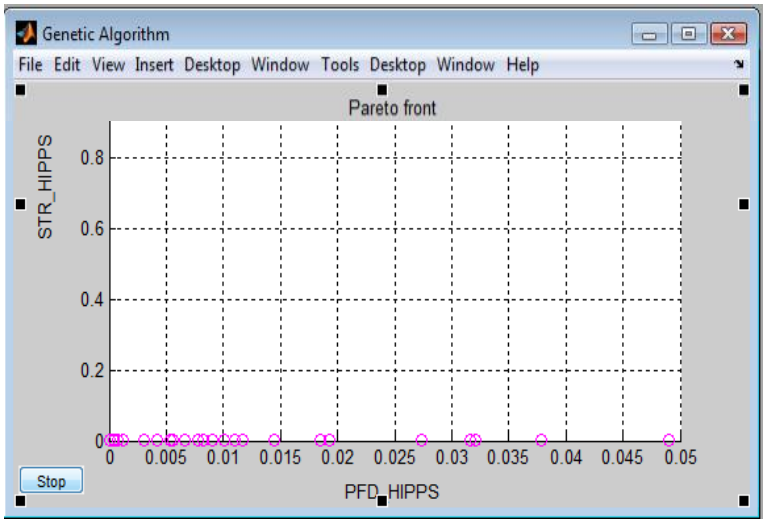

Figure 3.13: Front de Pareto (solutions non dominantes) relatif aux objectifs de PFD_{moy} et STR

3.4. Conclusion

La conception d'un *SIS* possédant une double performance, qui permet de satisfaire aux objectifs de sécurité et de disponibilité, représente un enjeu majeur pour les industriels. Dans cette optique, le troisième et dernier chapitre de ce document était consacré à l'optimisation d'un système instrumenté de sécurité qualifié de *HIPPS*. Pour ce faire, nous avons d'abord situé d'une manière précise le problème à optimiser : présentation des différents paramètres et variables entrant en jeu. Ensuite, la méthode des algorithmes génétiques, choisie pour résoudre ce problème, à été présentée. Nous rappelons, à ce titre, que l'utilisation d'une méthode exacte d'optimisation n'est pas envisageable dans notre cas de figure. Nous avons finalement étudié plusieurs stratégies d'optimisation, allant d'une simple procédure de minimisation de la PFD_{moy} jusqu'une optimisation multi-objectif complète et réaliste. L'aspect multi-objectifs considère une parfaite égalité entre les différentes grandeurs à optimiser, en l'occurrence : PFD_{moy}, STR_{moy} et les différents coûts d'achat et d'exploitation. Pour l'ensemble des stratégies étudiées, l'algorithme d'optimisation, implémenté dans l'outil «*Optimization Toolbox*» de l'environnement MATLAB, retourne des solutions qui répondent aux différentes contraintes imposées. Ceci confirme l'efficacité des algorithmes génétiques dans la résolution des problèmes difficiles et plus particulièrement l'optimisation des systèmes instrumenté de sécurité.

Conclusion générale

Nous proposons au niveau de cette conclusion générale de résumer l'essentiel des travaux présentés dans ce manuscrit. Aussi, quelques perspectives de recherche y sont exposées.

L'objectif de ce travail de recherche, rappelons-le, s'agissait d'abord de proposer une formulation analytique des performances des systèmes instrumentés de sécurité (*SIS*), vis-à-vis des objectifs de sécurité et de disponibilité, et d'établir ensuite une procédure d'optimisation des architectures des *SIS*. Pour cela, nous avons organisé le présent document comme suit.

Au niveau du premier chapitre, quelques éléments clés relatifs à la démarche d'analyse des risques ont d'abord été présentés. Ensuite, nous avons décrit brièvement le cadre organisationnel et technique des systèmes instrumentés de sécurité : la norme CEI 61508. Ces systèmes ont finalement été présentés en termes de définition, d'organisation et de fonctionnement.

Le second chapitre était consacré, dans un premier temps, à une étude bibliographique des différentes formulations analytiques relatives aux indicateurs de performance des *SIS* : PFD_{moy}, *PFH*, PFS_{moy} et *STR*. A cet effet, de différents documents ont été exploités. Pour chacun d'eux, nous avons souligné les différentes hypothèses simplificatrices. Aussi, un échantillon de résultats, pour les architectures 1*oo*2 et 2*oo*3, a été fourni à des fins de comparaison. Le second volet de ce chapitre était réservé à l'obtention des formules analytiques des PFS_{moy} et *STR* des différentes architectures *KooN*. Pour ce faire, nous avons mis à profit le formalisme des chaînes de Markov.

Finalement, le problème d'optimisation des architectures des *SIS* a été étudié au niveau du troisième chapitre. Nous avons, a ce titre, exposé ses différentes facettes, c'est-à-dire, l'ensemble des objectifs à respecter pour atteindre les spécifications liés à la sécurité de même que celles attachées à la disponibilité de production de l'installation surveillée. Un lien direct entre ces spécifications et les indicateurs de performance précédents a été établi. Nous avons ensuite présenté la méthode d'optimisation adoptée : les algorithmes génétiques. Cette méthode a montré son efficacité pour la résolution de problèmes dits difficiles : espace de recherche très vaste, domaine de recherche non continu. *In fine*, nous avons exploré plusieurs stratégies d'optimisation, en augmentant progressivement la difficulté du problème. Parmi celles-ci, la procédure d'optimisation multi-objectifs permet d'attribuer le même poids aux comportements dangereux (PFD_{moy}) et sûr (*STR*), ainsi qu'aux coûts d'achat et de maintenance. C'est elle qui répond le plus aux attentes des industriels. Il convient de signaler que les solutions obtenues ne sont pas forcément les meilleures (*optima local*), toutefois elles respectent l'ensemble des contraintes établies.

Comme perspectives de recherche, nous souhaiterions généraliser l'approche d'optimisation, présentée au niveau du troisième chapitre, de telle sorte qu'elle pourrait intégrer des modèles analytiques (*AdD* et Chaînes de Markov) pour une évaluation réaliste des performances à optimiser. Cette intégration est justifiée par le fait que les formulations analytiques, en dépit de la facilité qu'elles offrent, ne permettent pas de rendre compte des performances des *SIS* pourvus d'architectures non usuelles (composants hétérogènes, tests échelonnés, durées entre tests différentes, …). Le second point d'amélioration consisterait à développer un outil logiciel d'optimisation des architectures des *SIS*. Ce fait permet une utilisation simplifiée et pratique de la procédure d'optimisation présentée au niveau du troisième chapitre.

ANNEXE: Fichier « *M.File* » de la fonction objectif relative à la *Stratégie* 1

Programmation de la *Stratégie* 1 : Minimisation de la PFD_{moy}^{HIPPS} sans aucunes contraintes.

```
function PFD_SIS = SIS_OPT (x)
if (fix(x(3))==1)
   LD_PT = 0.151E-6; DC_PT = 0.318; B_PT = 0.02; MTTRDD_PT = 4;
elseif (fix(x(3))==2)
    LD_PT = 1.9E-6; DC_PT = 0.51; B_PT = 0.02; MTTRDD_PT = 8;
else
    LD_PT = 4.11E-6; DC_PT = 0.1; B_PT = 0.05; MTTRDD_PT = 10;
end
LDD_PT=DC_PT*LD_PT; LDU_PT = (1-DC_PT)*LD_PT; BD_PT=B_PT/2;
A =(factorial (abs(fix(x(1)))))/(factorial(abs(fix(x(2))-1)))*
(x(3)/x(3))*((1-B_PT)*LDU_PT + (1-BD_PT)*LDD_PT)^(fix(x(1))-
fix(x(2))+1);
j=1:(fix(x(1))-fix(x(2))+ 1);
if (fix(x(4))==1)
   T1_PT=4380;
 elseif (fix(x(4))==2)
   T1_PT=8760;
 elseif (fix(x(4))==3)
   T1_PT =13140;
else
  T1_PT =17520;
end
MDT_PT_IND =
(x(4)/x(4))*(LDU_PT/(LDU_PT+LDD_PT))*((T1_PT./(j+1))+MTTRDD_PT)+
(LDD_PT/(LDU_PT+LDD_PT))*MTTRDD_PT;
PMDT_PT_IND = prod(MDT_PT_IND);
PFD_PT_IND=A*PMDT_PT_IND;
PFD_PT_CCF=B_PT*LDU_PT*((T1_PT/2)+MTTRDD_PT)+BD_PT*LDD_PT*MTTRDD
_PT;
PFD_PT =PFD_PT_IND+PFD_PT_CCF;
if (fix(x(7))==1)
   LD_LS = 0.01E-6; DC_LS = 0.9; B_LS = 0.01; MTTRDD_LS = 4;
elseif (fix(x(7))==2)
    LD_LS = 10E-6; DC_LS = 0.9; B_LS = 0.01; MTTRDD_LS = 8;
else
    LD_LS = 15E-6; DC_LS = 0.67; B_LS = 0.01; MTTRDD_LS = 8;
end
LDD_LS=DC_LS*LD_LS; LDU_LS = (1-DC_LS)*LD_LS; BD_LS=B_LS/2;
B =(factorial(abs(fix(x(5)))))/(factorial(abs(fix(x(6))-1)))*
(x(7)/x(7))*((1-B_LS)*LDU_LS + (1-BD_LS)*LDD_LS)^(fix(x(5))-
fix(x(6))+1);
k=1:(fix(x(5))-fix(x(6))+ 1);
if (fix(x(8))==1)
   T1_LS=8760;
 elseif (fix(x(8))==2)
   T1_LS =13140;
else
  T1_LS =17520;
end
```

```
MDT_LS_IND =
(x(8)/x(8))*(LDU_LS/(LDU_LS+LDD_LS))*((T1_LS./(k+1))+MTTRDD_LS)+
(LDD_LS/(LDU_LS+LDD_LS))*MTTRDD_LS;
PMDT_LS_IND = prod(MDT_LS_IND);
PFD_LS_IND=B*PMDT_LS_IND;
PFD_LS_CCF=B_LS*LDU_LS*((T1_LS/2)+MTTRDD_LS)+BD_LS*LDD_LS*MTTRDD
_LS;
PFD_LS =PFD_LS_IND+PFD_LS_CCF;
if (fix(x(11))==1)
   LD_SDV = 3.35E-6; DC_SDV = 0.25; B_SDV = 0.02; MTTRDD_SDV =
8;
elseif (fix(x(11))==2)
   LD_SDV = 5.44E-6; DC_SDV = 0.20; B_SDV = 0.05; MTTRDD_SDV =
8;
else
   LD_SDV = 7.9E-6; DC_SDV = 0.1; B_SDV = 0.1; MTTRDD_SDV = 10;
end
LDD_SDV=DC_SDV*LD_SDV; LDU_SDV = (1-DC_SDV)*LD_SDV;
BD_SDV=B_SDV/2;
C =(factorial(abs(fix(x(9)))))/(factorial (abs(fix(x(10))-1)))*
(x(11)/x(11))*((1-B_SDV)*LDU_SDV + (1-
BD_SDV)*LDD_SDV)^(fix(x(9))-fix(x(10))+1);
l=1:(fix(x(9))-fix(x(10))+ 1);
if (fix(x(12))==1)
   T1_SDV=2190;
 elseif (fix(x(12))==2)
   T1_SDV =4380;
 elseif (fix(x(12))==3)
   T1_SDV =8760;
 elseif (fix(x(12))==4)
   T1_SDV =13140;
else
  T1_SDV =17520;
end
MDT_SDV_IND =
(x(12)/x(12))*(LDU_SDV/(LDU_SDV+LDD_SDV))*((T1_SDV./(l+1))+MTTRD
D_SDV)+(LDD_SDV/(LDU_SDV+LDD_SDV))*MTTRDD_SDV;
PMDT_SDV_IND = prod(MDT_SDV_IND);
PFD_SDV_IND=C*PMDT_SDV_IND;
PFD_SDV_CCF=B_SDV*LDU_SDV*((T1_SDV/2)+MTTRDD_SDV)+BD_SDV*LDD_SDV
*MTTRDD_SDV;
PFD_SDV =PFD_SDV_IND+PFD_SDV_CCF;
PFD_SIS = PFD_PT+PFD_LS+PFD_SDV;
```

Références Bibliographiques

[3SF, 1974] Société pour l'avancement de la sécurité des systèmes en France. *Terminologie cohérente dans le domaine de la sécurité moderne*. *Document non publié.*

[CEA, 2002] Commissariat à l'Energie Atomique (CEA). *Méthode Organisée et Systémique d'Analyse des Risques.* CEA, France.

[CEI 61508, 2009] Norme CEI 61508, nouvelle version. Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité. Parties 1 à 7, 2009. *Commission Electrotechnique Internationale,* Genève, Suisse.

[CEI 61508-1, 1998] Norme CEI 61508. Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Parties 1: Prescriptions générales - Edition 1.0 - Décembre 1998-2002. *Commission Electrotechnique Internationale*, Genève, Suisse.

[CEI 61508, 1998] Norme CEI 61508. Sécurité fonctionnelle des systèmes électriques / Électroniques / électroniques programmables relatifs à la sécurité – Parties 1 à 7, octobre 1998-2000. *Commission Electrotechnique Internationale*, Genève, Suisse

[CEI 61508-4, 1998] Norme CEI 61508. Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Parties 4: Définitions et abréviations - Edition 1.0 - Décembre 1998-2002. *Commission Electrotechnique Internationale*, Genève, Suisse.

[CEI 61508-5, 1998] Norme CEI 61508. Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Parties 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité - Edition 1.0 - Décembre 1998- 2000. *Commission Electrotechnique Internationale,* Genève, Suisse.

[CEI 61508-6, 1998] Norme CEI 61508. Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité – Parties 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3 -- Edition 1.0 - Décembre 1998- 2010. Commission Electrotechnique Internationale, Genève, Suisse.

[CEI 61511-1, 2003]. Sécurité fonctionnelle – Systèmes instrumentés de sécurité pour le secteur des industries de transformation – Partie 1: Cadre, définitions, exigences pour le système, le matériel et le logiciel - Edition 1.0 - Janvier 2003. *Commission Electrotechnique Internationale*, Genève, Suisse.

[CEI 61511, 2003] Norme CEI 61511. Sécurité fonctionnelle - Systèmes instrumentés de Sécurité pour le domaine de la production pour processus – Parties 1 à 3, janvier 2003-juillet 2003. Commission Electrotechnique Internationale, Genève, Suisse.

[CEI 61508-5, 1998] Norme CEI 61508-5. Annexe B. Concepts d'ALARP et de risque Tolérable. Commission Electrotechnique Internationale, Genève, Suisse.

[CHARPENTIER, 2002] Philippe charpentier. architecture d'automatisme en securite des machines: Etudes des conditions de conception liées aux défaillances du mode commun – Thèse de DOCTEUR de l'Institut Nationale Polytechnique de LORRAINE – Spécialité Automatique.

[CCPS, 2001] Layer of protection analysis; simplified process assessment; center for chemical process safety of the American institute for chemical Engineers;New York;2001.

[Desroches, 1995] Desroches A. Concepts et méthodes probabilistes de base de sécurité. Lavoisier ; France ; 1995.

[DIN V 19250, 1994] Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Berlin, Deutsches Institut für Normung.

[DUTUIT et al. 2009] Yves DUTUIT, Fares INNAL, Geert DECONINCK etude complementaire des systemes instrumentes de securite - Rapport TOTAL 2009_version finale, l'ADERA (Association pour le Développement de l'Enseignement et des Recherches auprès des universités, des centres de recherche et des entreprises d'Aquitaine).

[ECKART ZITZLER *et al.,* 2002] Eckart Zitzler, Marco Laumanns and Stefan Bleuler. *A Tutorial on Evolutionary Multiobjective Optimization*. Swiss Federal Institute of Technology (ETH) Zurich, Computer Engineering and Networks Laboratory (TIK), Switzerland.

[ELEGBEDE, 2003] Elegbede C. and Adjallah K. *Availability allocation to repairable systems with genetic algorithms: a multiobjective formulation*. *Reliability Engineering and System Safety*, 82, p.319-330.

[GRIF, 2011] Manuel utilisateur GRIF-2011-Markov.pdf (téléchargeable à partir du site: http://grif-workshop.com/downloads/user-manuals/).

[GOBLE, 1998] Goble W.M. *Control Systems Safety Evaluation & Reliability*. 2nd Edition, 515 pages, ISA. Research Triangle Park, North Carolina 27709, USA.

[HOUTERMANS, 2006] Houtermans M.J.M. *Spurious Trip Levels-How To Design Plants That are Safe and Do Not Trip*, (White Paper). RISKNOWLOGY GmbH, Zug, Switzerland.

[HSE, 1995] Health and Safety Executive. *Out of control (why control systems go wrong and how to prevent failure)*. HSE Books, ISBN 07176 08476.

[IDDIR, 2009], Olivier IDDIR Evaluation de la probabilité de défaillance des Mesures de Maîtrise des Risques (MMR), SE 4 057. Technique de l'ingénieur.

[ILO-OSH, 2001] *ILO-OSH 2001. Guidelines on occupational safety and health management systems*. BIT.

[INERIS, 2003] INERIS-DRA35. *Outils d'analyse des risques générés par une installation industrielle*. INERIS, Direction des Risques Accidentels. France.

[INNAL, 2008] FARES INNAL. Contribution à la modélisation des systèmes instrumentés de sécurité et à l'évaluation de leurs performances Analyse critique de la norme CEI 61508, Thèse de Docteur de L'Université BORDEAUX 1.

[INNAL, 2011] INNAL Farés. *Modélisation des systèmes industriels et évaluation de leurs performances en termes de sécurité et de disponibilité de production.* Mémoire d'Habilitation Universitaire, Institut d'Hygiène et Sécurité Industrielle-Université de Batna, Novembre 2011.

[ISA, 2002] ISA-TR84.00.02–Part 2. Safety Instrumented Functions (SIF)–Safety Integrity Level (SIL) Evaluation Techniques. Part 2: Determining the SIL of A SIF via Simplified Equations. ISA. Research Triangle Park, North Carolina 27709, USA.

[ISO, 1999] ISO/CEI Guide 51. *Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes.* Organisation internationale de normalisation (ISO).

[ISO, 2002] ISO/CEI Guide 73. *Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes.* Organisation internationale de normalisation (ISO).

[ISO 31000, 2009] ISO 31000 : 2009. *Management du risque –Principes et lignes directrices*. Organisation internationale de normalisation (ISO).

[LANTERNIER ET ADJADJ, 2008] Lanternier B. et Adjadj A. Allocation de Niveau d'Intégrité de Sécurité (Sil) Requis conformément à la Norme CEI 61511- Institut Nationale de l'Environnement Industriel et des Risques, DCE/LEEL Verneuil en Halatte – France – Publié dans la Revue internationale sur l'Ingénierie des Risques Industriels Vol 1, No 1

[LE MOIGNE, 1984] J. L. Le Moigne. La théorie du système général – Théorie de la modélisation. *PUF*, Paris, France.7

[LIEVENS, 1976] C. Lievens. Sécurité des systèmes. *Cepadues éditions*, Toulouse, France.

[LUTTON, 2009] Évelyne LUTTON. *Algorithmes génétiques et algorithmes évolutionnaires*. Techniques de l'Ingénieur, S 7 218.

[MARSEGUERRA *et al.*, 2006] Marseguerra M., Zio E. and Martorell S. *Basics of genetic algorithms optimization for RAMS applications*. Reliability Engineering and System Safety, 91, p. 977–991.

[MATLAB, 2009] MATLAB, version R2009b. The MathWorks, Inc: www.mathworks.com.

[OHSAS, 1999] OHSAS 18001. Système de management de la santé et de la sécurité au travail - Spécification. BSI, AFNOR.

[PAGES et *al*. 1980] A. Pages et M. Gondran. Fiabilité des systèmes. Editions Eyrolles. Collection de la DER de EDF. Paris. France.

[PORTMANN et OULAMARA ; 2009] Marie- Claude portmann, Ammar oulamara .Optimisation discrète. Dossier délivré pour commun de la documentation 09/02/2009.

[SALLAK, 2007] Sallak Mohamed. *Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité*. Thèse de Doctorat de l'Institut National Polytechnique de Lorraine.

[SALLAK *et al.* 2008] Sallak M., Aubry J.F and Simon C. *Conception optimale des systèmes instrumentés de sécurité : une approche par les Blocs diagrammes de fiabilité*. MOSIM 08, 7ème Conférence Internationale de Modélisation, Optimisation et Simulation des Systèmes, Paris, France.

[SINTEF, 2006] Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook, 2006 Edition. SINTEF, Trondheim, Norway.

[SINTEF, 2010] Rapport SINTEF. Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition.

[STARRY, 2009] Patrick STARRY. « Application des méta-heuristiques d'optimisation en électronique », Dossier délivré pour commun de la documentation 09/02/2009. Technique de l'ingénieur.

[TIENNTO et al. 2008] tiennto r. chaabi y. et bertho p. Etude et Certification d'un Système Instrumenté de Sécurité sous marin – 16ème Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement - Avignon 6-10 octobre 2008, communication 6B-4.

[TORRES-ECHEVERRÍA *et al.*, 2009] Torres-Echeverría A.C., Martorell and S. Thompson H.A. *Design optimization of a safety-instrumented system based on RAMS+C addressing IEC61508 requirements and diverse redundancy*. Reliability Engineering and System Safety, 94, p.162-179.

Résumé

Vérifier l'aptitude du SIS à exécuter correctement ses fonctions constitue une étape très importante pour sa validation. La conception des SIS assurant une double performance : satisfaire aux objectifs de sécurité et de disponibilité, constitue une tâche d'importance capitale.

Avec le souci majeur de la maîtrise du risque, et partant de la norme CEI 61508 comme document normatif de référence pour la mise en œuvre des SIS, ensuite une étude des formulations mathématiques des indicateurs de performance (PFD_{moy}, PFH, PFS_{moy}, STR) en vue d'une comparaison simplifiée des différentes approches, l'objectif de ce travail est de vérifier l'adéquation des formulations analytiques existantes ayant trait à la PFS_{moy} et le STR. Ainsi, nous proposons une nouvelle formulation mathématique basée sur les chaînes de Markov, formalisme qui permet une modélisation comportementale effective des systèmes testés périodiquement. Le problème d'optimisation expose les différents facteurs et critères. Ceci a été réalisé à travers un exemple réaliste issu de l'industrie de procédés, en utilisant comme outil les algorithmes génétiques (AG). En application, plusieurs stratégies de maintenance ont été testées, d'une stratégie simpliste (minimisation de la PFD_{moy} sans aucune contrainte) à une stratégie plus complexe (optimisation multi-objectifs).

***Mots Clés**: Sécurité Industrielle, Gestion des Risques, SIS, Norme CEI 61508, Performances, Optimisation, Modélisation.*

Summary

To verify the faculty of SIS to execute its functions correctly constitutes an important step for its validation. The conception of SIS assuring a double performance: to satisfy to the objectives of security and availability, constitutes a fundamental importance task.

With the major worry of the mastery of the risk and hence of the norm CEI 61508 as normative document of reference for the stake some performances in view of a comparison simplified of the different approaches. The objective of this research is to verify the adequacy of the existing analytic formulations having milked in the PFDmea and the STR. We propose a new mathematical formulation based on the chains of Markov, formalism that permits one, modeling effective compartmental of the systems tested periodically. The problem of optimization exposes the different factors and criteria's. It will be achieved through a realistic example descended of the industry of the proceeded while using like tools the genetic algorithms as applying five strategies of maintenance has been tested; of a simplistic strategy (minimization of the PFDmea without any constraint) to a strategy more complex (multi-objectives optimization).

***Key words**: Industrial Safety, Risk Management, SIS, Norm CEI 61508, Performances, Optimization, Modeling*