RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

École Nationale Polytechnique

Département : Maîtrise des Risques Industriels et Environnementaux

Filière : QHSE-GRI

Entreprise : General Electric

Mémoire de Master en QHSE-GRI

Conception optimale d'un Système Instrumenté de Sécurité
- Cas stations de coating de GE Oil & Gas ALGESCO -

Racha DJEBBAR

Sous la direction de :	M. Badreddine BOUSBAÏ	EHS Manager
	M. Mohamed Boubakeur	Maître-assistant
	M. Bouzid BENKOUSSAS	Professeur

Présenté et soutenu publiquement le 21/06/2017

Composition du Jury :

Président	M. Abdelmalek CHERGUI	Professeur	ENP
Rapporteurs	M. Badreddine BOUSBAÏ	Manager EHS	GE
	M. Mohamed Boubakeur	Maître-assistant	ENP
	M. Bouzid BENKOUSSAS	Professeur	ENP
Examinateurs	M. Amin BENMOKHTAR	Maître-assistant	ENP
	M. M'hamed BOUSBAI	Maître-assistant	ENP
	M. Salah LARBI	Professeur	ENP

ENP 2017

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

École Nationale Polytechnique

Département : Maîtrise des Risques Industriels et Environnementaux

Filière : QHSE-GRI

Entreprise : General Electric

Mémoire de Master en QHSE-GRI

Conception optimale d'un Système Instrumenté de Sécurité
- Cas stations de coating de GE Oil & Gas ALGESCO -

Racha DJEBBAR

Sous la direction de :	M. Badreddine BOUSBAÏ	EHS Manager
	M. Mohamed Boubakeur	Maître-assistant
	M. Bouzid BENKOUSSAS	Professeur

Présenté et soutenu publiquement le 21/06/2017

Composition du Jury :

Président	M. Abdelmalek CHERGUI	Professeur	ENP
Rapporteurs	M. Badreddine BOUSBAÏ	Manager EHS	GE
	M. Mohamed Boubakeur	Maître-assistant	ENP
	M. Bouzid BENKOUSSAS	Professeur	ENP
Examinateurs	M. Amin BENMOKHTAR	Maître-assistant	ENP
	M. M'hamed BOUSBAI	Maître-assistant	ENP
	M. Salah LARBI	Professeur	ENP

ENP 2017

Dédicaces

Je dédie ce travail à :

Mes parents et Zakaria,

Ma tante et ma cousine Khadidja,

Mes sœurs Ilhem, Aicha, Lynda et mon frère Chakib,

Mes sœurs et amies Marya, Anissa, Souad et Leïla

Mon enseignant Mohamed Meddah

Toute ma famille et tous mes amis

Toute personne qui m'est chère.

Racha

Remerciements

Nos remerciements s'adressent tout d'abord à ALLAH Le Tout Puissant pour la force qu'il nous a donnés pour atteindre nos objectifs et arriver où nous en sommes.

Nos remerciements s'adressent également aux membres du jury, Monsieur CHERGUI, Professeur à l'ENP, qui nous fait l'honneur de présider ce Jury, Monsieur BENMOKHTAR, Monsieur BOUSBAÏ ainsi que Monsieur LARBI enseignants à l'ENP, qui ont bien voulu accepter d'examiner et de juger ce travail.

Nous souhaiterions adresser nos vifs remerciements aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire :

À Monsieur B. BOUSBAÏ, notre promoteur de l'entreprise, pour nous avoir faits confiance et mis à notre disposition toutes les ressources nécessaires pour l'accomplissement de notre mission. Pour son encadrement, ses remarques ainsi que ses précieux conseils durant toute la période du stage où nous avons pu bénéficier de sa riche expérience et savoir-faire. Pour son accueil, sa bienveillance, sa patience et son savoir-être, qui ont toujours suscités notre profond respect.

À Monsieur M. BOUBAKEUR, maître-assistant à l'ENP, pour sa disponibilité, ses précieux conseils et son aide qui a contribué à l'exceptionnel encadrement dont nous avons bénéficiés.

À monsieur B. BENKOUSSAS, professeur à l'ENP, pour ses conseils et sa confiance en nous qui nous ont motivés à nous surpasser dans la réalisation de ce rapport.

Nos remerciements s'adressent également à toute l'équipe de GE Oil & Gas ALGESCO, avec qui, ce fut un plaisir de travailler avec. Une pensée particulière à Madame N. BELADJAL, Monsieur N. LADJALI, Monsieur B. MADJADJI, et Monsieur T. HOCINI pour leur disponibilité et leur veille au meilleur déroulement de notre travail.

Un remerciement particulier à monsieur F. TAMSSAOUET, ingénieur QHSE-GRI pour son aide, sa patience et aussi ses conseils dans la réalisation de ce travail.

Sans oublier Monsieur R. BOURDJOUL, pour son dévouement, son aide et ses nombreux services.

Notre gratitude se destine également aux enseignants du Département QHSE-GRI de l'Ecole Nationale Polytechnique qui ont contribué à notre formation et notre suivi durant notre passage.

À toutes les personnes qui ont contribuées de près ou de loin à la réalisation de ce travail, nous présentons notre respect et notre gratitude.

ملخص: الهدف من هذا العمل هو تصميم البنية المثلى لنظام السلامة المجهز المقترحة لتحقيق الأهداف الأمنية التي أعرب عنها SIL والمطلوبة من نظام الامدادات بوقود الكيروزين من محطة الطلاء الحراري في شركة ALGESCO. نقلنا مشكلة التصميم الأمثل لنظام السلامة المجهز إلى مشكلة التقليل من التكاليف الإجمالية تحت قيود الـ SIL المطلوب والمعبر عنها بدلالة موثوقية SIS. قمنا أولا بنمذجة SIS بواسطة BdF. ثم استخدمنا الخوارزمية الجينية لتحسين هيكل BdF وأيضا للحصول على الترتيب الأمثل لـ SIS. في الأخير قمنا باستعمال شجرة الفشل الضبابية لتقييم الـ SIL الحقيقي المتعلق بالترتيب الأمثل المحصل عليه.

كلمات البحث: SIL ، الأمثل، الخوارزمية الجينية، الرسوم البيانية الضبابية للموثوقية، شجرة الاحتمالات الضبابية،

Abstract: The purpose of this study is to design an optimal architecture of an Instrumented Safety System. This system was proposed in order to achieve the safety objectives that showed the required SIL of a kerosene supply system from a coating station of ALGESCO Company. The SIS optimal design problem has been reduced to a problem of its global cost minimization under the constraint that required SIL will be depending on SIS reliability. Firstly, we have modeled the SIS using Reliability Blocks Diagram (RBD). Then, a Genetic Algorithm has been used to optimize the RBD structure and obtain optimal configurations of the SIS. Finally, we evaluated the real SIL of the optimal configuration obtained using a fuzzy fault tree.

Key Words : SIS, Optimisation, Reliability, Genetic Algorithme, Reliability Diagram Blocs, Fuzzy Fault tree analysis.

Résumé : Le but de ce travail est de concevoir une architecture optimale d'un Système Instrumenté de Sécurité proposé pour atteindre les objectifs de sécurité exprimés par le SIL requis d'un système d'alimentation en kérosène d'une station de coating à l'entreprise ALGESCO. Nous avons ramené le problème de conception optimale du SIS à un problème de minimisation de son coût global sous contrainte du SIL exigé qui est exprimé en fonction de la fiabilité du SIS. Nous avons d'abord modélisé le SIS par des Blocs diagrammes de Fiabilité (BdF). Ensuite, nous avons utilisé un Algorithme Génétique pour l'optimisation de la structure du BdF et l'obtention de configurations optimales du SIS. Enfin, nous avons évalué, par un Arbre de Défaillance Flou, le SIL réel de la configuration optimale obtenue.

Mots-clefs : SIS, Optimisation, Fiabilité, Algorithmes génétiques, Blocs de diagrammes de Fiabilité, Arbre de Défaillance Flou

Table des matières

Liste des tableaux

Liste des figures

Liste des abréviations

AG	Algorithmes Génétiques
BdF	Blocs diagrammes de Fiabilité
E/E/EP	Electrical / Electronic / Electronic Programmable
IEC	International Electronic Comission
MDS	Méthode du Diagramme de Succès
PFD	Probabilité de défaillance à la demande
PFH	Probabilité et de défaillance dangereuse par heure
SdF	Sûreté de fonctionnement
SIF	*Safety Instrumented Function*
SIL	Security Integrity Level (niveau d'intégrité de sécurité)
SIS	Systèmes Instrumentés de Sécurité

Introduction générale

Dans le cadre de la conception des SIS, les fiabilistes assignent aux SIS la réalisation des objectifs de sûreté de fonctionnement dès la phase d'expression du besoin en réduction de risque. Cet assignement a pour but, d'une part, d'aider le concepteur à rationaliser ses choix de composants et, d'autre part, de garantir à l'exploitant les objectifs de sûreté de fonctionnement exigés.

Si nous considérons le SIS à réaliser se décomposant successivement en sous-systèmes, ensembles et composants, nous sommes amenés à procéder, dès la phase de faisabilité, à la distribution des objectifs au niveau sous-systèmes, puis au niveau ensembles jusqu'au niveau composants.

Cette distribution des objectifs intervient dans une logique descendante visant à allouer aux composants les exigences de sûreté de fonctionnement exprimées au niveau système et, dans une logique ascendante visant à consolider au niveau système les prévisions de données de sûreté de fonctionnement exprimées à des niveaux inférieurs.

La distribution des objectifs de sûreté de fonctionnement paraît donc indispensable pour:

- Pouvoir exprimer les exigences de sûreté de fonctionnement au niveau des composants.
- Vérifier que les principes retenus (architecture, concepts technologiques, etc.) sont compatibles avec les exigences de sûreté de fonctionnement émises par les fiabilistes.
- Procéder à la comparaison des concepts envisageables dans l'optique d'une optimisation du coût. Il est certain qu'une stratégie de conception, dont le souci est purement technique, permet d'atteindre les objectifs de sûreté de fonctionnement, mais elle le fait au détriment du coût de conception. Par contre, si la stratégie de conception cherche uniquement à réduire le coût de conception, le résultat est un nombre important de défaillances dangereuses et le non-respect des objectifs.

Il est donc primordial de trouver une stratégie d'allocation des objectifs de sûreté de fonctionnement au niveau des composants du SIS qui permette d'établir le meilleur compromis entre le coût de conception du SIS et les objectifs de sûreté de fonctionnement qui sont exprimés sous forme du SIL requis.

Dans nos travaux, le problème de conception des SIS est ramené à un problème de minimisation du coût global du SIS sous contrainte du SIL exigé. Le SIL est exprimé en fonction de la fiabilité du SIS. La conception optimale du SIS se fait donc par le choix

du nombre et des types de composants dans chaque sous-système du SIS qui garantissent un coût global minimal et le SIL exigé.

Le présent mémoire est scindé en trois chapitres.

Dans le premier chapitre, des généralités sur la notion de sécurité et la sécurité fonctionnelle sont présentées. La seconde partie de ce chapitre s'intéresse aux systèmes instrumentés de sécurité, leurs types de redondance et la modélisation des architectures sur lesquelles ils peuvent se présenter.

Dans le deuxième chapitre, nous expliquerons le concept ainsi que la méthodologie de l'optimisation par les algorithmes génétiques, qui représente l'une des approches les plus utilisées pour résoudre le problème d'optimisation des SIS.

Dans le troisième chapitre et qui concerne la partie pratique de notre travail, nous présentons le SIS sur lequel nous allons travailler et dont le SIL requis est connu. Ensuite, nous appliquerons les algorithmes génétiques pour optimiser la conception de ce SIS. Enfin, nous appliquerons la méthode de l'arbre de défaillance flou pour évaluer le SIL réel du SIS optimisé.

Chapitre 1. Notions théoriques sur la Sûreté de Fonctionnement (SdF)

Chapitre 1. Notions théoriques sur la Sûreté de Fonctionnement (SdF)

1.1. Introduction

Les industriels s'occupent des performances des systèmes en termes de sécurité. Les moyens qu'ils mettent en œuvre pour réduire les risques sont nombreux et variés. De ce fait, la conception du procédé ainsi que le choix des équipements participent principalement à la réduction du risque.

De plus, diverses sécurités sont également installées. Ces types de sécurités, appelés barrières de sécurité, utilisent des moyens qui contribuent à la prévention ou à la protection afin de minimiser les conséquences d'un dysfonctionnement.

Dans ce chapitre, nous allons introduire dans un premier temps quelques concepts relatifs à la sécurité et à la sûreté de fonctionnement. Nous nous intéresserons par la suite aux Systèmes Instrumentés de Sécurité et la modélisation de leurs architectures.

1.2. Quelques concepts de la SdF

- **Sûreté de fonctionnement SdF**

Aptitude d'une entité à satisfaire une ou pluseurs fonctions requises dans des conditions données. On notera que ce concept peut englober la fiabilité, la disponibilité, la maintenabilité, la sécurité, la durabilité... ou des combinaisons de ces aptitudes.

Au sens large, la SdF est considérée comme la science des défaillances et des pannes.

- **Risque**

Événement redouté évalué en terme de fréquence et de gravité. En sûreté de fonctionnement, il s'agit d'identifier les événements indésirables, d'évaluer la fréquence de leurs survenues et de quoi elle dépend, d'évaluer la gravité de leurs survenues et de quoi elle dépend ; de prendre ses décisions en fonction de leurs impacts sur le triplet « événement, fréquence, gravité » qu'on appelle risque.

- **Sécurité**

La sécurité est souvent définie par son contraire : elle serait l'absence de phénomènes dangereux, de risque inacceptable, d'accident ou de sinistres (Exida, 2005).

Selon (Desroches, Leroy, & Vallée, 2003), la sécurité concerne *la non occurrence d'événements pouvant diminuer ou porter atteinte à l'intégrité du système, pendant toute la durée de l'activité du système, que celle-ci soit réussie, dégradée ou ait échouée.*

Et suivant le guide (ISO/CEI 73, 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.*

Dans le cadre des installations industrielles, la sécurité consiste à la mise en œuvre des moyens évitant l'apparition de dangers. Elle s'énonce par l'absence de risque inacceptable, selon la norme (IEC 61508, 1998).

- **Sécurité fonctionnelle**

La sécurité fonctionnelle veille à contrôler l'absence de risques inacceptables qui pourraient :

- Engendrer des blessures ;
- Porter atteinte, directement ou indirectement, à la santé des personnes ;
- Dégrader l'environnement ;
- Altérer la propriété.

Selon la norme (IEC 61061, 1998), la sécurité fonctionnelle est *le sous-ensemble de la sécurité globale se rapportant à la machine et au système de commande de la machine qui dépend du fonctionnement correct des systèmes électriques de commande relatifs à la sécurité, des systèmes relatifs à la sécurité basés sur une autre technologie et des dispositifs externes de réduction de risque.*

Suivant la norme (IEC 61508, 1998), la sécurité fonctionnelle est *le sous-ensemble de la sécurité globale qui dépend du bon fonctionnement d'un système ou d'un équipement en réponse à ses entrées.*

- **Fiabilité R(t)**

Aptitude d'une entité à accomplir les fonctions requises dans des conditions données pendant une durée donnée.

Elle est caractérisée par la probabilité R(t) que l'entité accomplissant ces fonctions à l'instant 0 les accomplisse toujours à l'instant t.

C'est donc la probabilité de bon fonctionnement sur un intervalle de temps donné [0, t] et dans des conditions données.

Il résulte que la fiabilité, au sens mathématique du terme, correspond à un fonctionnement sans interruption sur une certaine période.

- **Taux de défaillance**

Le taux de défaillance, généralement noté $\lambda(t)$, est :

$$\lambda(t) = \frac{-dR(t)/dt}{R(t)} \qquad 1.1$$

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

- **Courbe en baignoire**

On constate souvent que la courbe représentant le taux de défaillance d'une série de composants en fonction du temps à la forme dite « courbe en baignoire » (figure 6.2).

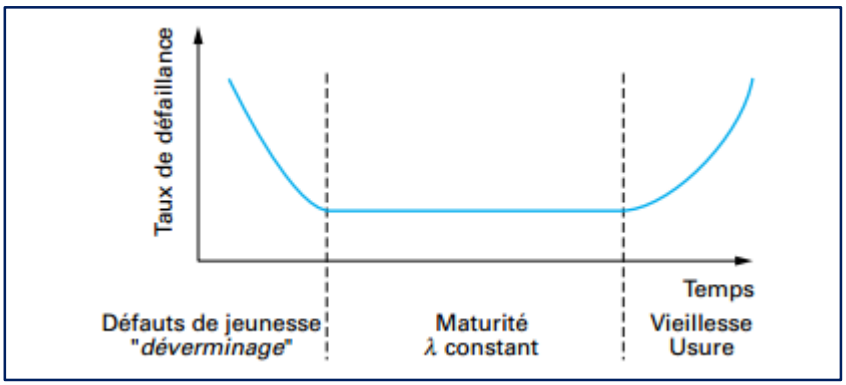

Figure 1.1. Taux de défaillance d'une série de composants : courbe en baignoire

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

Si cette évolution est connue, on arrête généralement l'utilisation de ces composants avant que cette remontée du taux de défaillance soit significative.

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

$$R(t) = e^{-\lambda t} \qquad 1.2$$

L'expérience a montré que, pour de nombreuses catégories de composants, il y avait une période assez longue entre la jeunesse et la vieillesse pendant laquelle cette hypothèse était une approximation tout à fait acceptable.

1.1. Norme IEC 61508

La norme internationale de sécurité IEC 61508 est une des dernières normes dédiées à la sécurité fonctionnelle. C'est un ensemble de règles et de recommandations permettant l'amélioration de la sécurité par l'utilisation des systèmes électriques, électroniques programmables E/E/EP. Cette norme orientée performances, propose une démarche opérationnelle permettant de mettre en place un système E/E/EP à partir de l'étude des exigences de sécurité issues notamment d'une analyse des risques. L'avantage de cette norme est qu'elle propose des moyens de justification sur l'ensemble du cycle de vie d'un produit en fonction du niveau de sécurité que l'on souhaite atteindre.

La norme (IEC 61508, 1998) se compose de sept volets comme suit :

- 61508-1 présente les définitions des prescriptions générales ;
- 61508-2 traite les prescriptions spécifiques aspect matériel des systèmes E/E/EP ;
- 61508-3 dédiée à la présentation des prescriptions spécifiques, aspect logiciel, des systèmes E/E/EP. Elle est développée dans la troisième partie de la norme ;
- 61508-4 présente les définitions et les abréviations utilisées ;
- 61508-5 donne des exemples de méthode pour la détermination des niveaux d'intégrité de sécurité ;
- 61508-6 fournit les guides d'application des parties 2 et 3 de la norme ;
- 61508-7 présente les techniques et les mesures recommandées lors de la validation des systèmes E/E/EP.

La complexité de la norme (IEC 61508, 1998) a conduit ses concepteurs à développer des normes relatives µa des secteurs bien précis (ex : machines, processus industriels, ferroviaire, centrales nucléaires...). La figure 6.4 montre la norme IEC 61508 générique ainsi que ses normes filles selon le secteur d'activité concerné. Elle influence le développement des systèmes E/E/EP et les produits concernés par la sécurité dans tous les secteurs (Sallak, 2008).

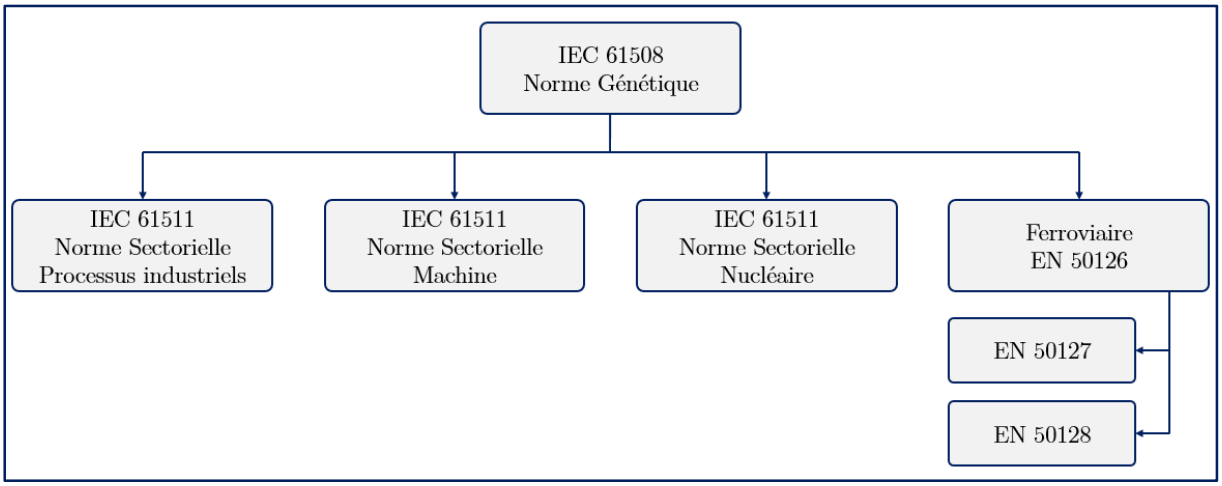

Figure 1.2. Normes sectorielles de la (IEC 61508, 1998)

1.2. Norme IEC 61511

(IEC 61511, 2000), s'intéresse à la sécurité fonctionnelle des SIS pour le secteur de l'industrie des procédés continus. Les remarques faites ci-dessus pour (IEC 61508, 1998) s'appliquent également à (IEC 61511, 2000). Cette norme est composée de trois grandes parties :

- 61511-1 présente les définitions et les exigences des systèmes (matériel et logiciel) ;
- 61511-2 traite les lignes directrices pour l'application de la première partie de la norme ;
- 61511-3 fournit des conseils pour la détermination des niveaux d'intégrité de sécurité ;

La (IEC 61511, 2000) détaille les définitions et les prescriptions relatives au cycle de vie en sécurité contenant la spécification, la conception, l'exploitation et la maintenance d'un système instrumenté de sécurité, fin de maintenir le procédé dans une position de sécurité convenable.

La norme (IEC 61511, 2000) est l'une des déclinaisons de la norme (IEC 61508, 1998). Les SIS constituent l'objet principal de ces deux normes, mais ils y sont considérés différemment selon les métiers auxquels elles s'adressent.

1.3. Concept des Systèmes Instrumentés de Sécurité

Les Systèmes Instrumentés de Sécurité (SIS) sont une composante essentielle des dispositifs de prévention des installations industrielles. Ils sont des combinaisons de capteurs, d'unité de traitement et d'actionneurs (équipements de sécurité) ayant pour

objectif de remplir une fonction ou sous-fonction de sécurité. Un SIS nécessite une énergie extérieure pour initier ses composants et mener à bien sa fonction de sécurité.

La norme (IEC 61511, 2000) définit les SIS de la façon suivante : *système instrumenté utilisé pour mettre en œuvre une ou plusieurs fonctions instrumentées de sécurité (SIF). Un SIS se compose de n'importe quelle combinaison de capteur(s), d'unités logique(s) et d'élément(s) terminal (aux).*

La norme (IEC 61508, 1998) définit quant à elle les systèmes relatifs aux applications de sécurité par : *un système E/E/EP (électrique/électronique/électronique programmable) relatif aux applications de sécurité comprend tous les éléments du système nécessaires pour remplir la fonction de sécurité.*

1.3.1. Constitution d'un SIS

Un SIS est composé de trois sous-fonctions principales reliées entre elles par des moyens de transmissions : **détection**, **traitement** et **actionnement**. Ces sous fonctions contribuent à assurer la sécurité fonctionnelle.

Figure 1.3. Structure d'un SIS

a. Détection (Sensor)

Cette sous-fonction est assurée par un ensemble d'éléments d'entrée (ex, capteurs, détecteurs) qui surveillent l'évolution des paramètres physico-chimiques représentatifs du comportement du procédé (température, pression, niveau…). Elle est constituée de deux éléments :

- **Le capteur** : l'élément responsable de la transformation d'une information physique en grandeur électrique adaptée au traitement.
- **Le transmetteur** : assure le conditionnement du signal émis par le capteur pour l'interface utilisateur. Le signal transmis peut être un signal analogique ou un signal de type binaire Tout ou Rien (1/0). Le transmetteur, suivant les cas (et ses possibilités), est connecté soit à l'entrée d'une unité de traitement, soit directement à un actionneur.

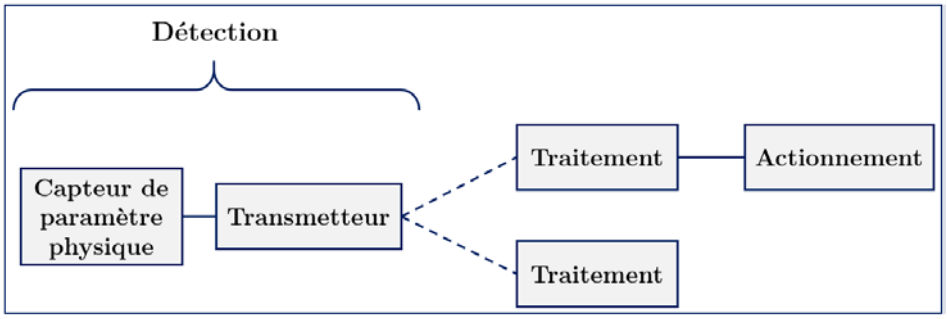

Figure 1.4. Architecture depuis le capteur jusqu'à l'actionneur (INERIS, 2008)

a. Traitement :

Cette sous-fonction fonction est assurée par une ou plusieurs unités logique LS (*Logic Solver*). Elle consiste à acquérir une grandeur mesurée par un capteur et à l'indiquer ou à activer la commande d'un ou plusieurs actionneurs à partir d'une fonction combinatoire des informations délivrées par différents capteurs. Le sous-système LS peut être un automate programmable ou un micro-ordinateur doté de logiciels spécifiques.

b. Actionnement :

Cette sous-fonction est assurée par un ou plusieurs actionneurs (ex, vanne, compresseur, alarme sonore et/ou visuelle …). Un actionneur agit directement (ex, vannes d'arrêt d'urgence) ou indirectement (ex, vannes solénoïdes) sur le procédé pour neutraliser sa dérive en mettant, en général, le système à l'arrêt (état sûr) au terme d'un délai qui doit être spécifié pour chaque fonction de sécurité.

Notons que plusieurs détecteurs et actionneurs peuvent être reliés à un ou plusieurs sous-systèmes LS.

1.2.1. Redondance au sein d'un SIS

Pour améliorer le niveau de confiance d'une barrière de sécurité, il est possible, entre autres, de la doubler totalement (redondance totale), ou de doubler une partie de ses composants (redondance partielle de la barrière de sécurité). À noter que la redondance peut être réalisée avec du matériel identique ou avec du matériel de technologie différente, ce dernier type de redondance permet de limiter les modes communs de défaillance.

Tous les éléments constituants une barrière de sécurité peuvent être redondés : capteurs, unité de traitement, actionneurs, éléments terminaux et même les moyens de transmission.

À noter que l'on peut distinguer plusieurs types de redondance :

- **Redondance active** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.
- R**edondance passive** qui est une redondance telle qu'une partie seulement des moyens d'accomplir une fonction requise est en fonctionnement, le reste n'étant utilisé sur sollicitation qu'en cas de défaillance de la partie en fonctionnement.
- **Redondance majoritaire m/n** qui est une redondance telle qu'une fonction n'est assurée que si au moins m des n moyens existants sont en état de fonctionner ou en fonctionnement.

Les architectures les plus souvent rencontrées relatives à ce dernier type de redondance sont les suivantes :

- **1oo1 (m=n=1)** : Cette architecture comprend un seul élément, et toute défaillance dangereuse de cet élément empêche le traitement correct de tout signal d'alarme valide.
- **1oo2 (m = 1 et n = 2)** : Cette architecture comprend deux éléments connectés en parallèle de façon que chacun puisse traiter la fonction de sécurité. Tant qu'un élément est opérationnel, la sécurité est garantie.
- **2oo2 (m = 2 et n = 2)** : Cette architecture comprend deux éléments connectés en parallèle de sorte qu'il est nécessaire que les deux éléments demandent la fonction de sécurité avant que celle-ci ne survienne. Il faut que les deux éléments soient opérationnels pour assurer la fonction de sécurité. La défaillance dangereuse d'un seul élément empêche le traitement correct de tout signal d'alarme valide.
- **2oo3 (m = 2 et n = 3)** : Cette architecture comprend trois éléments 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 élément donne un résultat différent des deux autres éléments. Tant que deux éléments sont opérationnels, la sécurité est garantie. Il faudrait la défaillance dangereuse de deux éléments pour qu'un signal d'alarme valide ne soit pas traité correctement.

Cette architecture représente aujourd'hui "l'état de l'art" car elle permet un bon compromis sécurité – disponibilité des outils de production.

1.2.2. Fonction Instrumentée de Sécurité

Une fonction Instrumentée de Sécurité (*Safety Instrumented Function* SIF) est une fonction réalisée par un système E/E/EP relatif à la sécurité, basée sur une autre technologie, ou par un dispositif externe de réduction de risque, prévue pour assurer ou

maintenir un état de sécurité de l'élément commandé par rapport à un événement dangereux spécifique.

Une SIF comporte un niveau d'intégrité de la sécurité spécifique nécessaire pour le maintien de la fonction de sécurité. Un SIS contient généralement plus qu'une SIF. Si les exigences d'intégrité de la sécurité pour ces SIF diffèrent, alors les exigences applicables au niveau d'intégrité de la sécurité le plus élevé s'appliquent au SIS. Pour une situation donnée, plusieurs fonctions de sécurité peuvent conduire à la réduction de la fréquence d'occurrence du danger (Mechri, 2011).

Une SIF est considérée comme une barrière de protection professionnelle lorsque le SIS est considéré comme un système réalisant une barrière de protection fonctionnelle, cette barrière est considérée comme une SIF (Mechri, 2011).

1.2.3. Paramètres de performance de sécurité des SIS

Deux indicateurs de la sécurité relatifs aux systèmes électroniques programmables dédiés aux applications de sécurité sont spécifiés par la norme (IEC 61508, 1998). Ils sont utilisés pour l'évaluation des performances des SIS suivant les deux modes de défaillances dangereuses et sûres. Ces indicateurs sont donnés sous forme de probabilité :

- Probabilité de défaillance à la demande (PFD) ;
- Probabilité et de défaillance dangereuse par heure (PFH).

1.2.3.1. Probabilité moyenne de défaillance à la demande PFD_{avg}

La probabilité de défaillance dangereuse à la sollicitation (*Probability of Failure on Demand* PFD) est la probabilité qu'un système ne puisse pas, sur un intervalle de temps [0 ; t], exécuter la fonction pour laquelle il a été conçu au moment où la demande de cette fonction est faite.

La probabilité moyenne de défaillance à la demande, notée PFD_{avg} (*Average Probability of Failure on Demand*) représente l'indisponibilité moyenne, sur un intervalle de temps [0 ; t], d'un système E/E/EP (Electrical / Electronic / Electronic Programmable) relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité.

1.2.3.2. Probabilité de défaillance dangereuse par heure

La probabilité d'une défaillance dangereuse par heure (*Probability of a dangerous Failure per Hour* PFH), est parfois appelée « fréquence des défaillances dangereuses », ou « taux de défaillances dangereuses », ou « nombre de défaillances dangereuses par heure ».

La PFH représente l'indisponibilité, sur un intervalle de temps [0 ; t], d'un système E/E/EP relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est fortement sollicité.

1.4. Modélisation des SIS

La conception optimale d'un SIS nécessite sa modélisation. Plusieurs approches sont utilisées selon le système à étudier et les critères d'analyse de défaillance fixés. Dans cette section, nous allons présenter l'approche que nous avons utilisées pour modéliser les SIS : les blocs diagrammes de fiabilité (BdF).

1.4.1. Concept

La méthode des blocs diagrammes de fiabilité est une des premières méthodes à avoir été utilisée pour analyser les systèmes et permettre des calculs de fiabilité (Villemeur, 1998). Elle est aussi appelée la Méthode du Diagramme de Succès (MDS).

C'est une représentation de la logique de fonctionnement des systèmes car elle est souvent proche de leur schéma fonctionnel. Cette méthode est basée sur l'utilisation de blocs pour représenter les composants, les sous-systèmes ou les fonctions. La modélisation consiste à rechercher les liens existant entre ces blocs. En outre, dans cette modélisation, les systèmes doivent vérifier les deux hypothèses suivantes :

- Hypothèse d'états binaires ;
- Indépendance des états de fonctionnement ou de défaillance des composants.

Les BdF sont ainsi utilisés dans de nombreux domaines industriels pour les systèmes non réparables (Dhillon & Yang, 1997), mais ils peuvent également, sous certaines conditions, être utilisés pour les calculs de fiabilité de systèmes réparables (Guo & Yang, 2006).

1.4.2. Diagramme série

La panne de l'un des éléments E_i du système entraîne la panne du système (figure 1.5). Si nous désignons par R_s la fiabilité du système et R_i la fiabilité du composant E_i, alors la fiabilité du système est donnée par :

$$R_s = \prod_{i=1}^{n} R_i \qquad 1.3$$

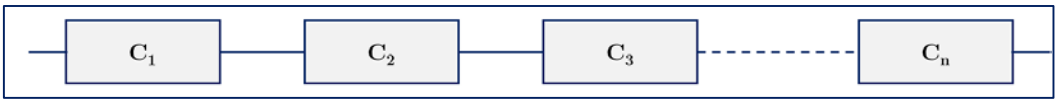

Figure 1.5. Représentation d'un diagramme série

1.4.3. Diagramme parallèle

La panne de tous les éléments Ei du système entraîne la panne du système (figure 1.6). Si un seul des éléments fonctionne alors il conduit au fonctionnement du système. Dans ce cas, la fiabilité du système est donnée par :

$$R_s = 1 - \prod_{i=1}^{n} (1 - R_i) \qquad 1.4$$

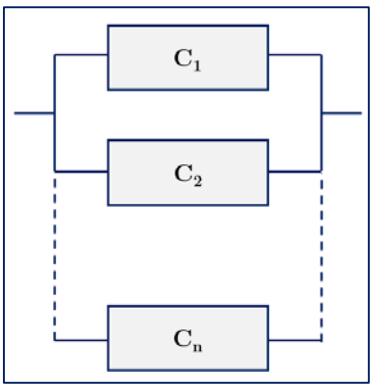

Figure 1.6. Représentation d'un diagramme parallèle

1.4.4. Diagramme en redondance k/n

Les systèmes à n composants qui fonctionnent si et seulement si au moins k de leurs composants fonctionnent, sont appelés des systèmes k parmi n (k/n) (figure 1.7).

On ne dispose pas d'une expression générale de la fiabilité d'un système k/n. Néanmoins, dans le cas où tous les composants du système ont la même fiabilité R, la fiabilité totale du système est donnée par :

$$R_s = \sum_{i=k}^{n} C_n^i R^i (1 - R)^{n-i} \qquad 1.5$$

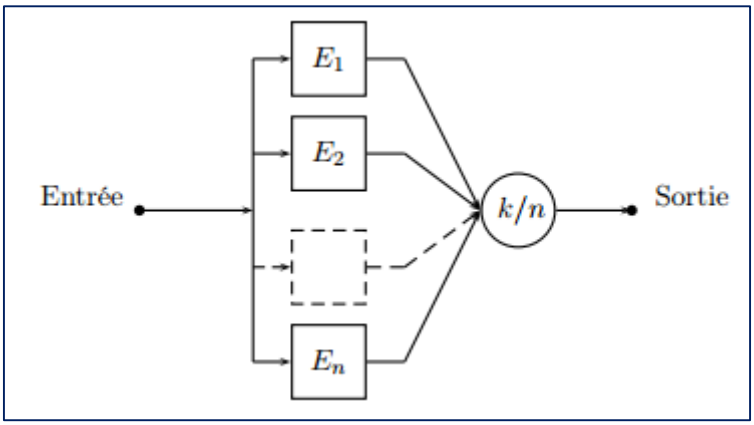

Figure 1.7. BdF d'un Système k/n

1.4.5. Diagramme complexe

Les diagrammes complexes sont des diagrammes qui ne peuvent pas être réduits à des combinaisons séries et/ou parallèles (VILLEMEUR, 1987).

Pour traiter les diagrammes complexes (figure 1.8), nous pouvons utiliser :

- Les liens minimaux et les coupes minimales.
- La fonction de structure.
- Le théorème des probabilités totales.
- La table de vérité.

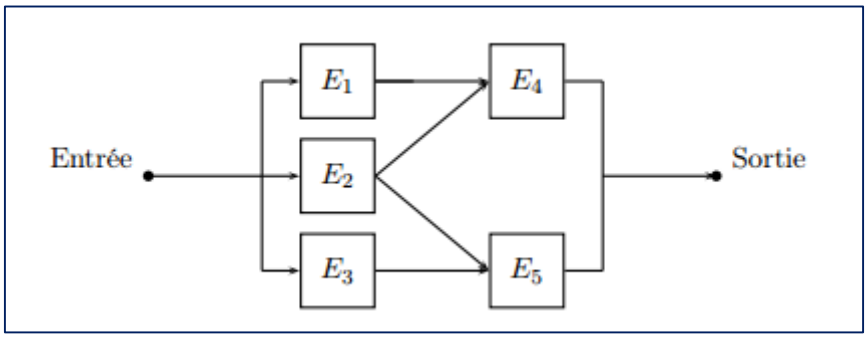

Figure 1.8. Schéma de connexion d'un système complexe

1.4.6. Liens minimaux et coupes minimales

Dans un schéma de connexion, un lien est un ensemble de blocs dont le fonctionnement assure le succès de la mission du système. Un lien minimal est une des plus petites combinaisons de blocs qui lorsqu'ils sont en fonction permettent d'assurer la fonction requise pour le système (il ne contient pas d'autres liens).

Si Li est un lien minimal du système alors la fiabilité totale du système est donnée par :

$$R_s = P[\sum_{i=1}^{l} L_i] \quad 1.6$$

Où l est le nombre de liens minimaux du système.

Les coupes minimales représentent les plus petites combinaisons de défaillances des blocs qui compromettent la fonction requise pour le système.

Si Ci est une coupe minimale du système alors la fiabilité totale du système est donnée par :

$$R_s = 1 - P[\sum_{i=1}^{c} C_i] \quad 1.7$$

Où c est le nombre de coupes minimales du système.

1.4.7. Calcul flou des fiabilités

Pour le calcul des fiabilités, nous allons suivre la loi exponentielle. Cette dernière est la loi suivie par la variable aléatoire t lorsque le taux de défaillance est constant $\lambda(t) = \lambda$, où λ est une constante réelle strictement positive.

La fonction de fiabilité est définie pour tout $t \geq 0$, par : $R(t) = 1 - PFD_{avg} = e^{-\lambda t}$.

Dans notre application, l'étude sera faite pour un temps t=8766h et Les taux de défaillance sont déterminés des bases de données (OREDA, 2002)

Notons que les bases de données existantes ne donnent pas une valeur précise pour un taux de défaillance, mais un ensemble de valeurs selon les expériences faites sur l'équipement étudié, nous avons alors opté pour un calcul flou de la fiabilité, cela à partir des probabilités des défaillance à la demande calculés suivant la logique floue et suivant le modèle proposé par (Liang & Wang, 1993).

La fonction d'appartenance utilisée pour le calcul flou des fiabilités est de type triangulaire. Cette configuration permet de présenter les fiabilités des événements de base. (figure 1.9)

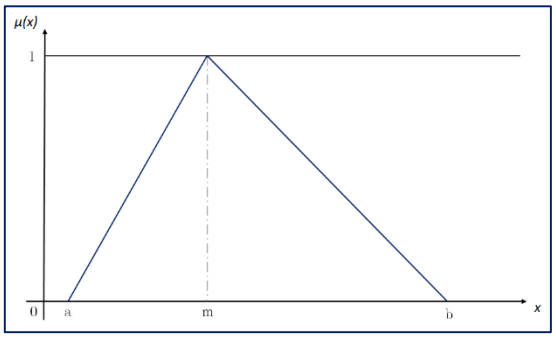

Figure 1.9. Fonction d'appartenance triangulaire

Telles que :

- a : limite inférieure de la probabilité donnée par les bases de données ;
- m : valeur moyenne de la probabilité donnée par les bases de données ;
- b : limite supérieure de la probabilité donnée par les bases de données.

Nous obtenons ainsi la probabilité moyenne de défaillance à la demande floue d'un composant A :

$$\widetilde{PFD_{avg}}(A) = (a, m, b) \tag{1.8}$$

Où la probabilité moyenne de défaillance à la demande ordinaire de :

$$PFD_{avg}(A) = \frac{a + b + c}{3} \tag{1.9}$$

Chapitre 2. Optimisation des Systèmes Instrumentés de Sécurité (SIS)

Chapitre 2. Optimisation des Systèmes Instrumentés de Sécurité (SIS)

2.1. Introduction

L'optimisation de la fiabilité est un domaine qui a suscité beaucoup d'intérêt de la part des chercheurs et des industriels à partir des années 60. En effet, la prise en compte de la fiabilité des composants lors de la conception des systèmes permet d'avoir une idée précise du coût et de la fiabilité totale du système.

Nous présentons dans ce chapitre une nouvelle approche de conception optimale des SIS pour l'obtention d'un SIL exigé. Nous ramenons le problème de conception optimale à un problème de minimisation du coût global du SIS sous contrainte du SIL exigé qui est exprimé en fonction de la fiabilité du SIS. L'approche optimale est basée sur l'utilisation des Blocs diagrammes de Fiabilité (BdF) et des Algorithmes Génétiques (AG).

Nous allons d'abord modéliser le SIS par un BdF. Nous utiliserons ensuite un AG pour l'optimisation de la structure du réseau de fiabilité et l'obtention de configurations optimales du SIS.

2.2. Méthodes d'optimisation

Pour augmenter la fiabilité d'un système, plusieurs méthodes peuvent être utilisées :

- Affectation de la fiabilité aux composants ;
- Ajout de composants en redondance ;
- Combinaison des deux techniques précédentes ;
- Affectation de composants interchangeables.

Chaque technique d'optimisation nécessite des ressources. La diversité des structures des systèmes, des contraintes sur les ressources et des options pour améliorer la fiabilité ont abouti à la construction et l'analyse de plusieurs modèles d'optimisation.

Kuo et al. (Kuo, Hwang, & Tillman, 2001) classent les méthodes d'optimisation de fiabilité selon :

- La structure des systèmes : séries parallèles, systèmes possédant une structure en réseaux, systèmes à redondance k parmi n, systèmes à structure indéfinie, etc.
- Le type de problème.

- Les techniques d'optimisation : heuristiques, méta heuristiques (algorithmes génétiques, recherche tabou, etc.), algorithmes exacts (programmation dynamique, méthodes du gradient, etc.) ou autres méthodes (décomposition, apportionment flou, etc.).

L'objectif de l'allocation de redondance est de déterminer une configuration optimale du système qui maximise sa fiabilité sous certaines contraintes (coût, poids, volume, etc.). Les variables de décision représentent le nombre de composants à placer en parallèle dans chaque sous-systèmedu système. En général, nous supposons que les composants sont identiques dans chaque sous-système. Les sous-systèmes étant montés en série.

Le problème d'allocation de redondance est exprimé sous la forme (P1) :

$$\textit{maximiser} \qquad R_s = f(x_1, \dots, x_n) \tag{2.1}$$

$$\textit{Sous les contraintes} \qquad g_i(x_1, \dots, x_n) \leq b_i, \qquad i = 1, \dots, m; \tag{2.2}$$

$$l_j \leq x_j \leq u_j, \qquad j = 1, \dots, m; \tag{2.3}$$

Où :

- R_s est la fiabilité du système.
- x_j est le nombre de composants en parallèle dans le sous-système j.
- n est le nombre de sous-systèmes du système.
- m est le nombre de ressources.
- $g_i(x_1, \dots, x_n)$ est la consommation de la ressource i par le système.
- l_j et u_j sont les bornes inférieure et supérieure de x_j.

Le problème d'allocation de redondance peut aussi s'exprimer sous la forme (P2) :

$$\textit{maximiser} \qquad R_s = f(x_1, \dots, x_n) \tag{2.4}$$

$$\textit{Sous les contraintes} \qquad \sum_{j=1}^{n} g_{i,j}(x_1, \dots, x_n) \leq b_i, \qquad i = 1, \dots, m; \tag{2.5}$$

$$l_j \leq x_j \leq u_j, \qquad j = 1, \dots, m; \tag{2.6}$$

$g_{i,j}(x_1, \dots, x_n)$est la consommation de la ressource i par le sous-système j. Les fonctions contraintes $g_{i,j}$ dans (P2) doivent être séparables pour chaque sous-système du système.

Pour résoudre les problèmes (P1) et (P2), plusieurs approches ont été introduites.

Les problèmes d'allocation de redondance se sont surtout focalisés sur les structures séries parallèles (Kuo, Hwang, & Tillman, 2001).

Dans de ce chapitre, nous allons nous focaliser sur l'optimisation par les algorithmes génétiques que nous avons utilisée. Nous allons d'abord justifier le choix des AG comme méthode d'optimisation dans nos travaux, puis nous allons introduire les principes de l'approche de conception optimale que nous avons proposée.

2.3. Algorithmes Génétiques (AG)

La résolution du problème de minimisation du coût global du SIS sous contrainte du SIL exprimé en fonction de la fiabilité du SIS n'est pas aisée. Pour résoudre ce type de problème, il existe diverses méthodes qui se divisent principalement en deux catégories : les méthodes déterministes et les méthodes stochastiques.

Les techniques stochastiques tournent principalement autour des algorithmes stochastiques d'évolution de populations (AG, recuit simulé, etc.), qui sont des méthodes d'optimisation globale. Elles sont robustes, parallélisables et permettent de déterminer l'optimum global d'une fonctionnelle. Leur inconvénient majeur réside dans le nombre important d'évaluations nécessaires pour obtenir l'optimum recherché. Les méthodes déterministes de type gradient présentent en revanche l'avantage de converger rapidement vers un optimum. Cependant, elles ne sont pas aussi robustes que les techniques stochastiques et, n'assurent pas que l'optimum déterminé est un optimum global. En outre, elles dépendent beaucoup du point de départ de recherche de l'extremum (Li & Aggarwal, 200).

Développés par Holland (Holland, 1975) à l'université du Michigan, les AG sont des méthodes d'optimisation de fonctions. Ces algorithmes s'inspirent de l'évolution génétique des espèces. Schématiquement, ils copient de façon extrêmement simplifiée certains comportements des populations naturelles. Ainsi, ces techniques reposent toutes sur l'évolution d'une population de solutions qui sous l'action de règles précises optimisent un comportement donné, exprimé sous forme d'une fonction, dite fonction sélective (fitness) (Michalewiez & Fogel, 2000).

2.3.1. Nomenclature des AG

Les AG étant basés sur des phénomènes biologiques, il convient de rappeler au préalable les termes utilisés dans les AG et leur signification biologique (tableau 2.1).

Tableau 2.1. Résumé de la terminologie utilisée en AG

Terme	AG	Signification biologique
Gène	Trait, caractéristique	Une unité d'information génétique transmise par un individu à sa descendance
Locus	Position dans une chaîne	L'emplacement d'un gène dans son chromosome

Allèle	Différentes versions d'un même gène	Une des différentes formes que peut prendre un gène
Chromosome	Chaîne	Une structure contenant les gènes
Génotype	Structure	L'ensemble des allèles d'un individu portés par l'ADN d'une cellule vivante
Phénotype	Ensemble des paramètres ou d'une structure décodée	Aspect physique et physiologique observable de l'individu obtenu à partir de son génotype.
Épistasie	Non linéarité	Terme utilisé pour définir les relations entre deux gènes distincts, lorsque la présence d'un gène empêche la présence d'un autre gène non allèle.

2.3.2. Avantage des AG

L'utilisation des AG présente plusieurs avantages :

- L'utilisation unique de l'évaluation de la fonction objectif sans se soucier de sa nature. En effet, nous n'avons besoin d'aucune propriété particulière sur la fonction à optimiser (continuité, dérivabilité, convexité, etc.), ce qui lui donne plus de souplesse et un large domaine d'application.
- Génération d'une forme de parallélisme en travaillant sur plusieurs points en même temps (population de taille N) au lieu d'un seul itéré dans les algorithmes classiques.
- L'utilisation des règles de transition probabilistes (probabilités de croisement et de mutation), contrairement aux algorithmes déterministes où la transition entre deux itérations successives est imposée par la structure et la nature de l'algorithme. Cette utilisation permet, dans certaines situations, d'éviter des optimums locaux et de se diriger vers un optimum global.

2.3.3. Inconvénients des AG

L'utilisation des AG présente aussi quelques inconvénients :

- Si l'AG nous garantit de trouver une bonne solution approchante, il ne nous garantit pas de trouver la valeur optimale.
- Suivant le problème, la résolution par l'AG peut être coûteuse en temps.

2.3.4. Concepts de base

Un AG est un algorithme itératif de recherche d'optimum, il manipule une population formée de points candidats appelés chromosomes. La taille constante de la population entraîne un phénomène de compétition entre les chromosomes. Chaque chromosome représente le codage d'une solution potentielle au problème à résoudre. Il est constitué d'un ensemble d'éléments appelés gènes, pouvant prendre plusieurs valeurs appartenant à un alphabet non forcément numérique (Ludovic, 1994).

À chaque itération, appelée génération, une nouvelle population est créée avec le même nombre de chromosomes. Cette génération consiste en des chromosomes mieux adaptés à leur environnement tel qu'il est représenté par la fonction sélective. Au fur et à mesure des générations, les chromosomes vont tendre vers un optimum de la fonction sélective. La création d'une nouvelle population à partir de la précédente se fait par application des opérateurs génétiques que sont : la sélection, le croisement et la mutation (Goldberg, 1994).

Ces opérateurs sont stochastiques. La sélection des meilleurs chromosomes est la première opération dans un AG. Au cours de cette opération l'algorithme sélectionne les éléments pertinents qui optimisent mieux la fonction. Le croisement permet de générer deux chromosomes nouveaux "enfants" à partir de deux chromosomes sélectionnés "parents", tandis que la mutation réalise l'inversion d'un ou plusieurs gènes d'un chromosome. La figure 2.1 illustre la séquence des opérations qui interviennent dans un AG de base (Ouarzizi, 1997).

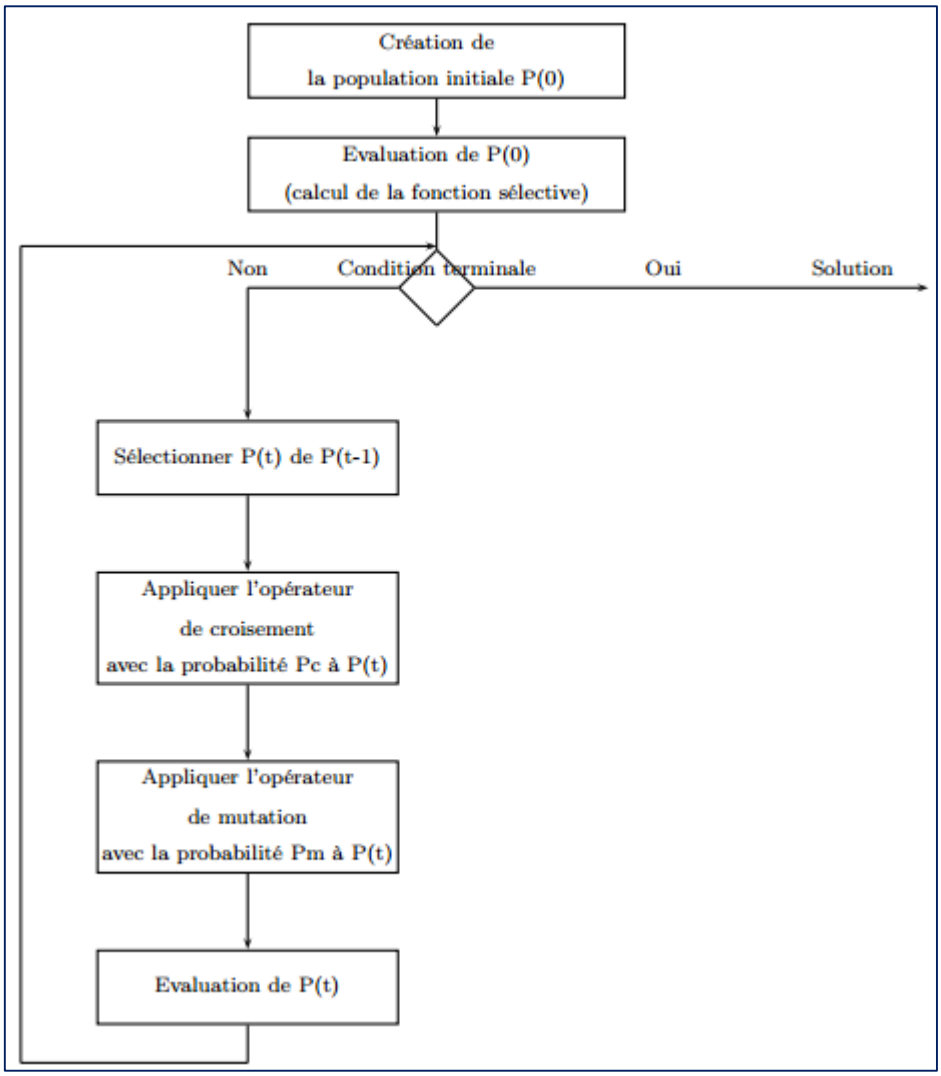

Figure 2.1. Algorithme génétique de base

2.3.5. Opérateurs des AG

Les opérateurs jouent un rôle prépondérant dans la possible réussite d'un AG. Nous en dénombrons trois principaux : la sélection, le croisement et la mutation. Si le principe de chacun de ces opérateurs est facilement compréhensible, il est toutefois difficile d'expliquer l'importance isolée de chacun de ces opérateurs dans la réussite de l'AG. Cela tient pour partie au fait que chacun de ces opérateurs agit selon divers critères qui lui sont propres (valeur sélective des individus, probabilité d'activation de l'opérateur, etc.). Nous détaillons par la suite les éléments de l'AG que nous avons utilisés.

2.3.5.1. Codage des solutions

Dans un AG, nous ne travaillons pas directement avec les données du problème mais avec une représentation de celles-ci appelées codage. La forme codée d'une solution est une chaîne qu'on appellera chromosome. Ce chromosome est à son tour constitué d'éléments qu'on appellera gènes.

Dans une population, nous parlerons indifféremment de chromosomes et d'individus. Le choix du codage dépend de la spécificité du problème traité. Il conditionne fortement l'efficacité de l'AG. Dans la littérature, nous trouvons trois types de codage :

- **Numérique** si l'alphabet est constitué de chiffres ;
- **Symbolique** si l'alphabet est un ensemble de lettres alphabétiques ou de symboles ;
- **Alphanumérique** si nous utilisons un alphabet combinant les lettres et les chiffres.

2.3.5.2. Population initiale

Une fois le codage choisi, une population initiale formée de solutions admissibles (chromosomes) du problème doit être déterminée. Plusieurs mécanismes de génération de la population initiale sont utilisés dans la littérature. La population initiale peut être générée aléatoirement, par duplication et évolution ou en s'appuyant sur une heuristique.

2.3.5.3. Taille des populations

Il n'y a pas de standardisation quant au choix de la taille des populations. Des tailles de population faibles augmenteront la vitesse de convergence de l'algorithme, mais aussi le risque de convergence prématurée vers des solutions non optimales. Des tailles de population trop grandes risquent au contraire de ralentir fortement la progression de l'algorithme. Cette importance de la taille est essentiellement due à la notion de parallélisme implicite qui implique que le nombre d'itérations de l'AG soit au moins proportionnelle au cube du nombre d'individus. La taille fréquemment utilisée est 30 (Michalewiez & Fogel, 2000).

2.3.5.4. Sélection

La sélection a pour objectif d'identifier les individus qui doivent se reproduire. Cet opérateur ne crée pas de nouveaux individus mais identifie les individus sur la base de leur fonction d'adaptation. Les individus les mieux adaptés sont sélectionnés alors que les moins bien adaptés sont écartés. Ceci permet de donner aux individus dont la valeur de la fonction sélective est plus grande une probabilité plus élevée de contribuer à la génération suivante. Vladimir (Vladimir, 2003) a souligné le fait que lorsqu'un AG est utilisé pour maximiser une fonction objective, dans certains cas, c'est le processus de sélection qui assure la convergence vers un optimum global. Il existe plusieurs types de sélection. Une des méthodes les plus connues est la roue de loterie biaisée (roulette wheel) de Goldberg (Goldberg, 1994).

2.3.5.5. Croisement

Le croisement a pour but d'enrichir la diversité de la population en manipulant la structure des chromosomes. Classiquement, les croisements sont envisagés avec deux parents et gênèrent deux enfants. Dans la littérature, plusieurs techniques de croisement sont utilisées dont les principaux sont le croisement barycentrique et le croisement à un ou plusieurs points (Michalewiez & Fogel, 2000). Le croisement à deux points est l'un des croisements les plus utilisés. Il consiste à couper le chromosome en deux points choisis aléatoirement et recombiner les morceaux en croisant les chromosomes.

Une probabilité de croisement P_C signifie que, quand deux parents sont candidats à la reproduction, nous tirons un réel x aléatoirement selon une loi uniforme sur l'intervalle [0,1], si x est inférieur à P_C, nous croisons alors les parents. Les valeurs généralement admises sont comprises entre 0,5 et 0,9 (Goldberg, 1994).

2.3.5.6. Mutation

L'opérateur de mutation permet d'introduire un facteur aléatoire dans les solutions générées, et d'élargir ainsi l'espace des solutions explorées (Goldberg, 1994) pour éviter à l'AG de s'enliser dans des optima locaux. Pour les codages en nombre réels, la mutation consiste à modifier légèrement quelques gènes des chromosomes. En général, on choisit une faible probabilité de mutation. Cette probabilité de mutation représente la fréquence à laquelle les gènes d'un chromosome sont mutés.

Par exemple, une mutation très utilisée est de tirer aléatoirement un seul gène dans le chromosome et à le remplacer par une valeur aléatoire avec une probabilité de mutation P_m. Cet opérateur est donc d'une grande importance. La probabilité de mutation P_m est généralement faible puisqu'un taux élevé risque de conduire à une solution sous-optimale. La mutation est traditionnellement considérée comme un opérateur marginal bien qu'elle confère aux AG la propriété d'ergodicité (i.e. tous les points de l'espace de recherche peuvent être atteints).

2.3.5.7. Remplacement

Cet opérateur est le plus simple, son travail consiste à réintroduire les descendants obtenus par application successive des opérateurs de sélection, de croisement et de mutation (la population P') dans la population de leurs parents (la population P).

Ce faisant, ils vont remplacer une certaine proportion de ceux-ci, proportion pouvant bien sûr être choisie. Le rapport entre le nombre d'individus nouveaux allant être

introduits dans la population P et le nombre d'individus de cette population est connu sous le nom de *generation gap*.

Nous trouvons essentiellement deux méthodes de remplacement différentes :

- **Le remplacement stationnaire :** dans ce cas, les enfants remplacent automatiquement les parents sans tenir compte de leurs performances respectives, et le nombre d'individus de la population ne varie pas tout au long du cycle d'évolution simulé, ce qui implique donc d'initialiser la population initiale avec un nombre suffisant d'individus.
- **Le remplacement élitiste :** dans ce cas, nous gardons au moins l'individu possédant les meilleures performances d'une génération à la suivante. En général, nous pouvons partir du principe qu'un nouvel individu (enfant) ne prend place au sein de la population que s'il remplit le critère d'être plus performant que le moins performant des individus de la population précédente. Donc les enfants d'une génération ne remplaceront pas nécessairement leurs parents comme dans le remplacement stationnaire et par conséquent la taille de la population n'est pas figée au cours du temps. Ce type de stratégie améliore les performances des AG dans certains cas. Mais présente aussi l'inconvénient d'augmenter le taux de convergence prématurément.

2.3.6. Choix des paramètres des AG

Comme pour toute heuristique d'optimisation, l'efficacité d'un algorithme génétique dépend du choix de ses paramètres (probabilités liées aux opérateurs d'évolution, taille des populations, etc.) qui gouvernent l'exploration des solutions et des conditions initiales. Il n'y a pas de règle générale pour le choix de ces paramètres. Pour qu'un AG ait des bonnes performances, il doit être exécuté plusieurs fois avec différentes tailles de population, probabilités de croisement et de mutation afin de trouver l'ensemble des paramètres qui conviennent le plus à l'utilisateur.

2.4. Conception optimale

Dans cette partie, nous présenterons une méthodologie proposée par Mecheri (Mechri, 2011) pour résoudre le problème de conception optimale des SIS. Ce problème a été ramené à un problème de minimisation du coût global du SIS sous contrainte du SIL exigé.

2.4.1. Pourquoi les AG ?

La première raison est que la mise en œuvre des AG ne nécessite aucune hypothèse ou information sur le système optimisé (pas de calcul de gradient par exemple), ce qui correspond à notre problématique où nous devons optimiser une fonction qui n'est pas connue à priori et qui n'est pas continue.

La deuxième raison est que les AG permettent un équilibre entre exploitation et exploration. Le mot équilibre est justifié par le fait que les deux procédures sont antagonistes. L'exploitation d'une direction de recherche consiste essentiellement à encourager l'apparition de ses représentants dans la population tandis que l'exploration plaide en faveur de nouvelles directions de recherche. L'AG apporte une solution à ce dilemme en allouant un nombre exponentiel croissant à la meilleure direction observée.

La troisième raison est que les AG ont montré de très bonnes performances dans la résolution de problèmes d'allocation de fiabilité et de redondance sur lesquels peu d'informations sont disponibles ou pour lesquels il faut considérer de multiples critères d'optimisation (Kuo, Hwang, & Tillman, 2001).

2.4.2. Méthodologie générale

Dans cette partie, nous présentons les différentes étapes de la méthodologie de conception optimale des SIS.

- **Définition de l'objectif SIL**

Lors de l'étude d'un process, quand il y a un danger éventuel, il faut procéder à une analyse de risques et dangers. Les risques existants y sont décrits et les mesures existantes et supplémentaires prises pour réduire ces risques y sont définies. Le risque subsistant doit toujours rester à un niveau tolérable. Après l'affectation des tâches de sécurité aux niveaux de protection, nous nous intéressons aux spécifications relatives aux exigences de sécurité pour les SIS. Ces exigences étant exprimées sous la forme d'un SIL. L'objectif est de concevoir le SIS pour qu'il puisse atteindre le SIL exigé.

- **Définition du SIS à proposer**

Pour chaque composant, nous disposons de son taux de défaillance et de son coût.

Rappelons qu'un SIS est généralement constitué de trois parties :

- Partie Détecteurs (D) ;
- Partie Unité de traitement (LS) ;

- Partie Actionneurs (A).

Chaque partie pouvant contenir plusieurs composants de différents types placés souvent en parallèle, notre objectif est de choisir les composants de chaque partie et leur connexion qui permettent d'atteindre le SIL exigé avec un coût global minimal.

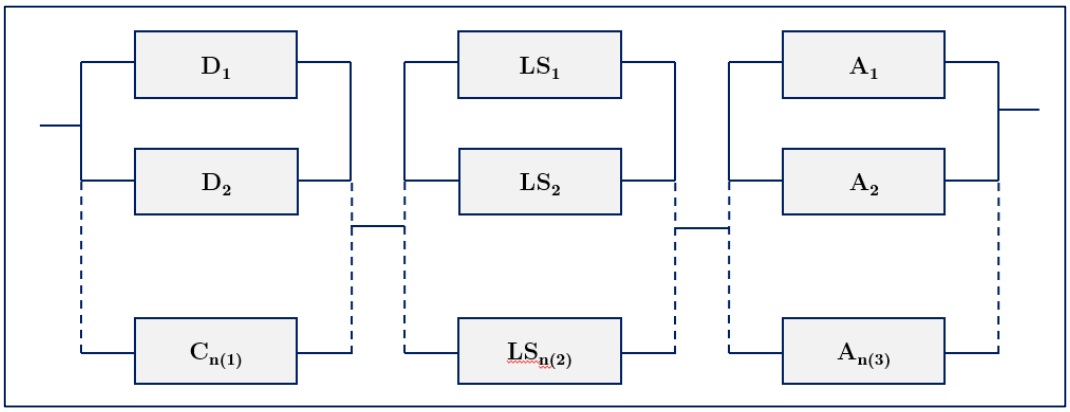

Figure 2.2. Blocs diagrammes de fiabilité général d'un SIS

- **Modélisation de la structure générale du SIS par un BdF**

Nous modélisons le SIS par bloc diagrammes de fiabilité défini sur l'ensemble n de ses composants :

$$n = \{D_1, D_2, \dots, D_{n(1)}, LS_1, LS_2, \dots, LS_{n(2)}, A_1, A_2, \dots, A_{n(3)}\}$$

Le composant D_i de la partie Détecteurs représente le Détecteur i. Conformément à la structure générale des SIS, le detecteur D_i ne peut être connecté qu'aux composants LS_i de la partie adjacente Unités de traitement. De même, les composants LS_i ne peuvent être connectés qu'aux composants A_i de la partie adjacente Actionneurs.

- **Codage des solutions et génération de la population initiale (configuration initiale du SIS)**

Nous cherchons les configurations optimales du bloc diagrammes de fiabilité du SIS (i.e., les connexions entre les différents composants du SIS) qui permettent d'atteindre les objectifs souhaités. Les chromosomes x (les solutions potentielles) sont des chaînes constituées de plusieurs gènes x_{ij}. Chaque chromosome représente une configuration particulière du BdF du SIS.

- **Calcul de la R_{SIS} et du coût du SIS**

La fiabilité du SIS R_{SIS} est calculée en fonction de la fiabilité de ses composants et du nombre de redondance dans chaque sous-système :

$$R_{SIS} = (1 - (1 - R_D)^{n(1)}) \times (1 - (1 - R_{LS})^{n(2)}) \times (1 - (1 - R_A)^{n(3)})$$

Où :

R_D	Fiabilité du détecteur.
R_{LS}	Fiabilité de l'unité logique.
R_A	Fiabilité de l'actionneur.
$n(1)$	Nombre de redondances dans la détection.
$n(2)$	Nombre de redondances dans le traitement.
$n(3)$	Nombre de redondances dans l'actionnement.

Le coût total du SIS est la somme des coûts des composants impliqués dans l'architecture optimale du SIS.

- **Calcul de la fonction objective**

Pour assurer les contraintes imposées par le respect du SIL, nous devons assurer que la fiabilité du SIS reste au-dessus d'une valeur minimale R_{min} et en dessous d'une valeur maximale R_{max}.

La fonction objective (fonction à optimiser), représente le coût du SIS, est donnée par :

$$coût = coût_D \times n(1) + coût_{LS} \times n(2) + coût_A \times n(3)$$

Où :

$coût_D$	Prix du détecteur.
$coût_{LS}$	Prix de l'unité logique.
$coût_A$	Prix de l'actionneur.

Le SIL requis représente la contrainte de cette optimisation, tel que, pour un niveau x du SIL, nous avons :

$$10^{-(x+1)} \leq PFD_{avg_{SIS}} < 10^{-x}$$

Ce qui implique :

$$1 - 10^{-(x+1)} \leq R_{SIS} = 1 - PFD_{avg_{SIS}} < 1 - 10^{-x}$$

- **Choix des paramètres de l'AG**

Comme pour toute heuristique d'optimisation, l'efficacité d'un algorithme génétique dépend du choix de ses paramètres (probabilités liées aux opérateurs d'évolution, taille des populations, etc.) qui gouvernent l'exploration des solutions, et des conditions initiales. Il n'y a pas de règle générale pour le choix de ces paramètres. Pour qu'un AG

ait des bonnes performances, Kimbrough a suggéré de l'exécuter plusieurs fois avec différentes tailles de population, probabilités de croisement et de mutation afin de trouver l'ensemble des paramètres qui conviennent le plus à l'utilisateur. C'est cette méthode que nous avons choisie.

- **Sélection**

La sélection permet d'identifier statistiquement les meilleurs chromosomes de la population et d'éliminer les moins bons. Dans notre cas, nous avons choisi la méthode de sélection du « *Uniform stochastic* » qui est aujourd'hui la technique de sélection la plus populaire en raison de sa simplicité et de son efficacité.

- **Croisement**

Nous avons choisi le croisement à deux points. Il consiste à couper le chromosome en deux points choisis aléatoirement et recombiner les morceaux en croisant les chromosomes. Une probabilité de croisement Pc signifie que, quand deux parents sont candidats à la reproduction, nous tirons un réel x aléatoirement selon une loi uniforme sur l'intervalle [0, 1].

- **Mutation**

La mutation choisie est une mutation très utilisée dont le principe est un tirage aléatoire d'un seul gène dans le chromosome et son remplacement par une valeur aléatoire.

- **Obtention d'une solution optimale**

En définissant un critère d'arrêt de l'AG, nous obtenons une solution optimale qui représente une configuration optimale du réseau de fiabilité du SIS.

Chapitre 3. Cas d'application

Chapitre 3. Cas d'application

3.1. Introduction

Dans cette partie, nous appliquerons la méthodologie de la conception optimale d'un SIS dont le SIL i est exigé.

Notre objectif est de concevoir le SIS dont le SIL i a été imposé au concepteur avec un coût total minimal. En conséquence, il faut choisir les composants de chaque sous système du SIS, ainsi que les connexions entre ces composants qui permettent d'obtenir le SIL exigé avec un coût de conception minimal. Notons que chaque composant ne peut être utilisé qu'une seule fois dans chaque partie du SIS.

À la fin du chapitre nous évaluerons le SIL réel de la configuration optimale obtenue.

3.2. SIS étudié

3.2.1. Système d'application du SIS

Le SIS étudié dans ce chapitre est proposé pour atteindre le niveau de SIL requis par un système d'alimentation de kérosène d'une station de revêtement thermique « coating » de l'entreprise GE Oil & Gas ALGESCO.

Le niveau de SIL requis par ce système a été évalué pour un niveau SIL 2, cela, dans une étude faisant l'objet d'un mémoire de fin d'étude sur la maîtrise des risques majeurs dans les stations de coating dans l'entreprise GE Oil & Gas ALGESCO. Le niveau de SIL a été évalué par la méthode graphe de risque floue.

3.2.2. Description du SIS

Une fuite du kérosène influe directement sur son débit de circulation pendant le fonctionnement de la machine. Afin de détecter une éventuelle fuite quand la station est en état de fonctionnement, Un suivi de l'évolution son débit doit être assuré depuis sa sortie du réservoir jusqu'à son entrée dans la cabine de coating. Pour ce faire, nous installerons un capteur de débit à la sortie du réservoir et un autre à l'entrée de la cabine.

Dans des conditions normales (sans fuite) le débit du kérosène reste constant tout au long du procédé. Le SIS proposé permet, en cas de différence entre les débits mesurés des deux capteurs, de couper l'alimentation en kérosène à la source et d'activer une alarme sonore pour prévenir le personnel de la situation.

3.2.3. Constitution du SIS 2

Ce SIS est composé de trois sous fonctions :

a. Détection :

Cette sous-fonction est assurée par un ensemble de deux capteurs de débit. Montés en série, ils permettent de surveiller le débit du kérosène tout au long du process. Ces capteurs de débit transforment l'information physique en grandeur électrique adaptée au traitement. Connectés à l'entrée d'une unité logique, ils permettent, par le biais de transmetteurs de débit, de lui transmettre cette information.

b. Traitement :

Cette sous-fonction est assurée par une unité logique (LS *Logic Solver*). Elle consiste à acquérir la grandeur mesurée par la sous-fonction « détection », à l'afficher sur le tableau de commande et à activer la commande de d'un actionneur « vanne d'isolement automatique », si les deux capteurs de débit indiquent deux informations différentes de débit.

c. Actionnement :

Cette sous-fonction est assurée par l'actionneur « vanne d'isolement automatique ». Le premier actionneur agit directement sur le système pour neutraliser sa dérive, en coupant l'alimentation en kérosène à la source par la fermeture d'une électrovanne placée à la sortie du réservoir du kérosène.

3.2.4. Architecture du SIS 2

La configuration de ce SIS est illustrée dans la figure 3.1. Cette structure a une configuration simple de type parallèle-série.

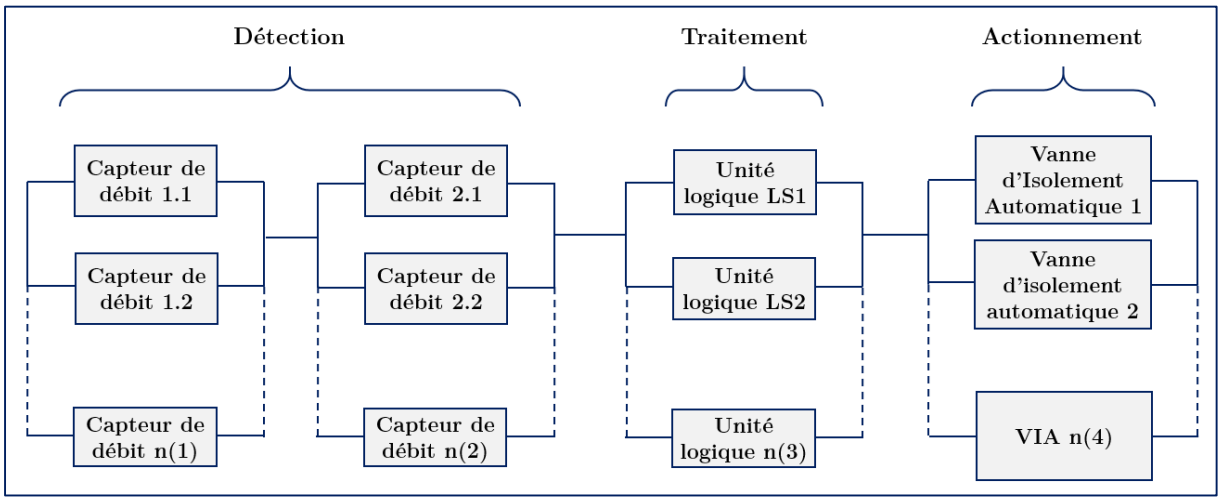

Figure 3.1. Architecture du SIS à optimiser

3.3. Formulation mathématique du problème

Ce problème de conception peut être ramené à un problème de minimisation du coût global du SIS sous une contrainte sur la fiabilité du SIS. La contrainte sur le SIL exigé est transformée en une contrainte sur la fiabilité du SIS selon les exigences de la norme (IEC 61511, 2000).

L'architecture permet de modéliser la fiabilité du SIS en fonction de la fiabilité de ses composants et le nombre de redondance dans chaque sous-système, telle que :

$$R_{SIS} = (1 - \left(1 - R_{D_1}\right)^{n(1)}) \times (1 - \left(1 - R_{D_2}\right)^{n(1)}) \times (1 - (1 - R_{LS})^{n(3)}) \times (1 - (1 - R_A)^{n(3)}) \quad 3.1$$

Où :

R_{SIS}	Fiabilité du SIS
R_{D_1}	Fiabilité du premier capteur de débit
R_{D_2}	Fiabilité du deuxième capteur de débit
R_{LS}	Fiabilité de l'unité logique
R_A	Fiabilité de la vanne d'isolement automatique

Sous la contrainte :

$$0{,}99 \leq R_{SIS} \leq 0{,}999$$

Le coût global du SIS est la somme des coûts de ses composants. En outre, pour notre étude nous avons pris une moyenne des prix en dollars des composants qui sont sur le marché :

$$Coût = 300 \times n(1) + 300 \times n(2) + 100 \times n(3) + 100 \times n(4) \quad 3.2$$

Les fiabilités obtenues à partir des probabilités de défaillance à la demande floues (chapitre 4, paragraphe 1.4.7) et les coûts des composants du SIS sont donnés dans le tableau 3.1.

Tableau 3.1. Paramètres des composants du SIS

Composant	PFD_{avg}	Fiabilité	Prix
Débitmètre	$2{,}4612.10^{-3}$	0,9975	500
Traitement logique	$9{,}2351.10^{-2}$	0,9076	100
Vanne d'isolement automatique	$3{,}7467.10^{-4}$	0,9806	100

Rappelons que la structure générale du SIS ainsi que les connexions éventuelles qui peuvent exister entre les différents composants sont données dans la figure 3.1.

Ainsi, le problème de conception revient à trouver la configuration (ou les configurations) optimale(s) (i.e., le choix des composants du SIS et les connexions entre ces composants) qui permet de :

- Minimiser « $Coût_{SYS}$ » ;
- Sous la contrainte : $0{,}99 \leq R_{SIS} < 0{,}999$

3.4. Résultats et analyse

Ayant défini toutes les données nécessaires (probabilités de défaillance et coûts des composants disponibles pour chaque sous-système du SIS) pour traiter le problème d'optimisation, l'étape suivante est l'implémentation de la procédure de conception optimale décrite précédemment (chapitre 2, paragraphe 2.4.2) pour le SIL exigé.

En ce qui concerne l'optimisation, nous avons utilisé le logiciel MATLAB r2017a et un processeur Intel(R) Core™ i7-7500U CPU @ 2.70 GHz 2.90 GHz. Les différents programmes d'optimisation ont été écrit sous MATLAB (Annexes 1) dont l'interface est illustrée sur la figure 3.2

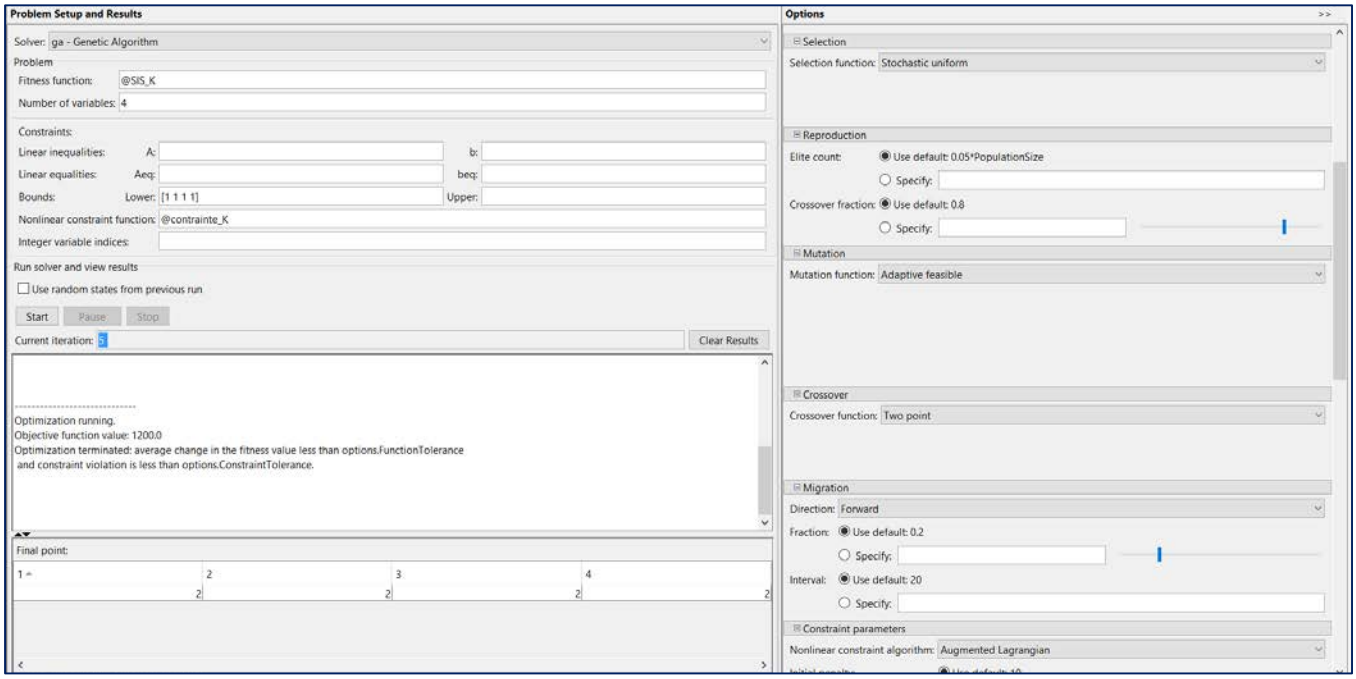

Figure 3.2. Interface de l'environnement des AG dans MATLAB

Le résultat obtenu est représenté par le vecteur : [2, 2, 2, 2]. L'architecture de ce SIS est présentée dans la figure 3.3.

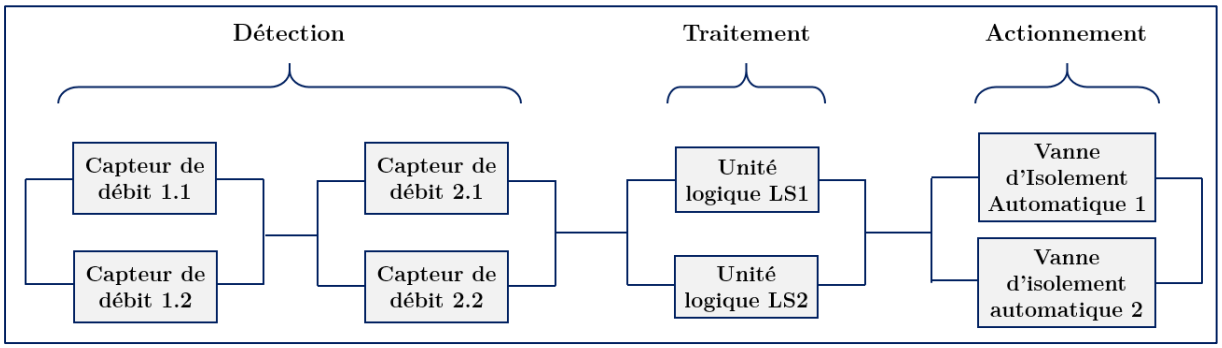

Figure 3.3. Architecture optimale du SIS étudié

Le prix de ce SIS donné par la fonction objective est égale à 2400 $.

3.5. Évaluation des SIL

L'évaluation du niveau d'intégrité de sécurité d'un SIS est déterminée par des méthodes qualitatives et quantitatives. Elles permettent ; d'examiner les différents dangers provenant du système opérationnel et de déterminer le SIL de la SIF pour réduire la criticité du danger analyse. L'objectif global de ces méthodes est de d'écrire une procédure d'identification des SIF, d'établir les niveaux de sécurité correspondant et de les mettre en œuvre dans un SIS afin de ramener le procède dans l'état de sécurité attendue. Dans notre cas, nous allons utiliser la méthode Arbre de Défaillance Flou (AdD Flou).

3.6. Arbre de Défaillance Flou

La méthode des arbres de défaillance est l'une des méthodes les plus utilisées dans les analyses des performances des SIS. Elle a pour objectif le recensement des causes entrainant l'apparition de l'évènement indésirable d'un système et le calcul de sa PFD_{avg}. Elle constitue un moyen de représentation de la logique des défaillances, cette méthode est adaptée aussi pour l'étude des systèmes élémentaires présentant des défaillances de mode commun.

L'arbre de défaillances est une méthode déductive, qui commence par l'évènement indésirable et détermine ses causes. L'analyse par l'arbre de défaillances nécessite deux phases ; une qualitative, où on détermine la fonction logique du système en terme de l'ensemble de ses coupes minimales, et l'autre est dite quantitative, où on calcule la probabilité d'occurrence de l'évènement indésirable (sommet).

L'évaluation quantitative de la probabilité de l'évènement sommet qui représente la déflabilité du système lorsque cet évènement est la défaillance d'un système non réparable. La méthode de l'arbre de défaillances consiste à rechercher toutes les combinaisons possibles d'évènements entrainant la réalisation de l'évènement indésirable.

On représente graphiquement ces combinaisons au moyen d'une structure arborescente dont l'évènement non désire est le sommet (ou racine).

Pour d'écrire la relation entre les évènements et la logique d'un système, l'arbre de défaillances utilise des portes logiques. Ces portes indiquent les types des évènements et les types de relation qui sont impliquées.

L'arbre de défaillances peut mener à des évaluations quantitatives de la probabilité d'occurrence de l'évènement indésirable qui représente la déflabilité lorsque cet évènement est la défaillance d'un SIS non réparable.

3.6.1. Quantification de l'AdD

L'AdD permet d'évaluer la probabilité moyenne de défaillance de l'événement-sommet à partir de celles des événements de base, telles que :

- La probabilité de défaillance d'un évènement de sortie A de la porte ET (généré si et seulement si toutes les entrées Ai de la porte sont présentes) est égale à :

$$PFD_{avg}(A) = \prod_{i=1}^{n} PFD_{avg}(A_i) \qquad 3.3$$

- La probabilité de défaillance d'un évènement de sortie A de la porte OU (généré si et seulement une ou plusieurs entrées Ai de la porte sont présentes) est égale à:

$$PFD_{avg}(A) = 1 - \prod_{i=1}^{n} (1 - PFD_{avg}(A_i)) \qquad 3.4$$

En appliquant ces deux règles, les probabilités des événements intermédiaires jusqu'à celle de l'événement-sommet sont calculées à partir des probabilités des événements de base et des conditions seulement.

Tel que, la probabilité de défaillance d'un événement Ai suit la loi exponentielle et est égale à :

$$PFD_{avg}(A_i) = 1 - e^{-\lambda_i t} \qquad 3.5$$

Où t est le temps de mission alloué à la simulation des défaillances étudiées. Dans notre cas, le calcul est fait pour une période d'une année, soit : t=8766h.

- **Calcul flou**

Afin de prendre en compte les incertitudes sur les probabilités de défaillance, nous avons opté pour l'utilisation de la logique floue. Cette dernière permet de traduire la dispersion

des probabilités des bases de données par des intervalles de probabilités avec une valeur moyenne.

Dans nos calculs, nous allons utiliser l'arbre de défaillance flou proposé par Liang et Wang (Liang & Wang, 1993) (chapitre 1, paragraphe 1.4.7)

3.6.2. Application de l'AdD sur le SIS étudié

Pour la construction de cet arbres de défaillance et pour le calcul des PFD_{avg}, nous avons utilisé le logiciel « *Arbre Analyste version 2.2.0* » ; logiciel spécifique à l'analyse des performances de sûreté de fonctionnement par calculs d'arbres de défaillances.

Les PFD_{avg} calculées à partir des taux de défaillances déterminées de la base de donnée (OREDA, 2002) (voir tableau 3.1) sont introduite dans le logiciel. Les détails de calcul sont dans l'annexe 2.

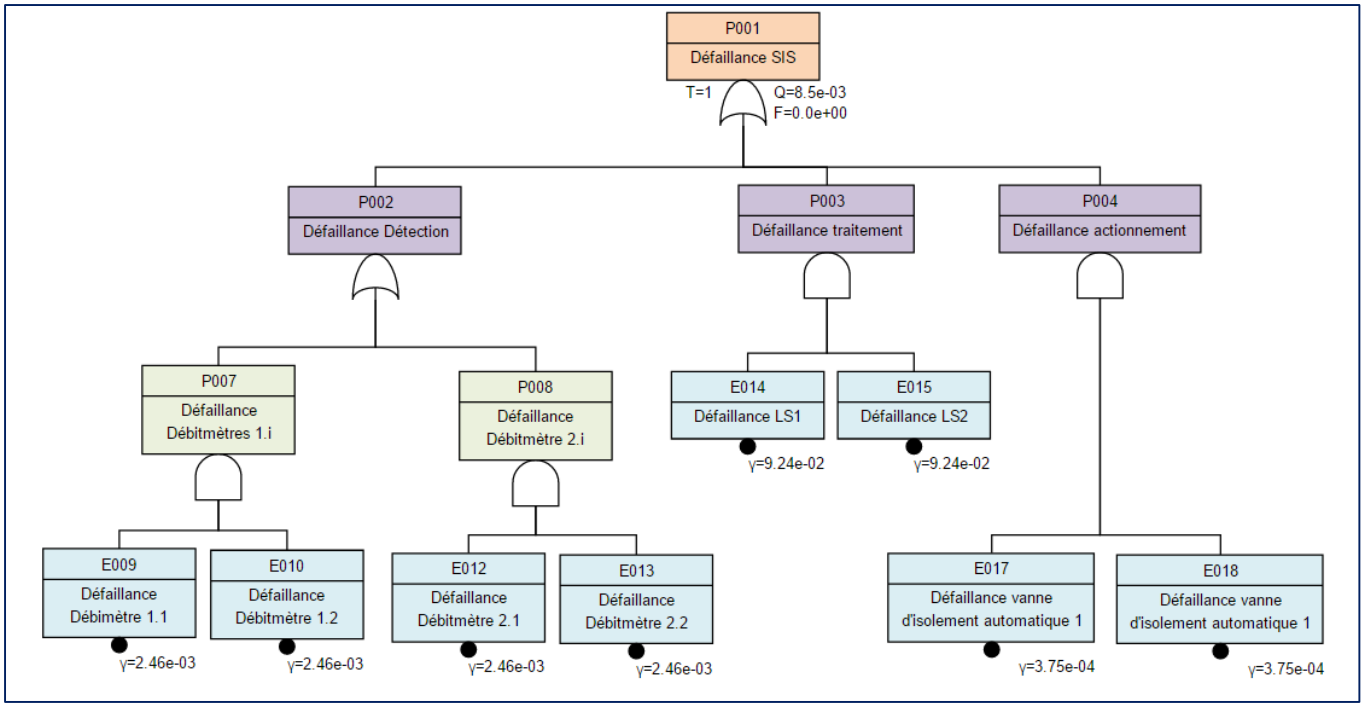

Figure 3.4. AdD d'une défaillance d'un SIS

Le logiciel a permis de déterminer une probabilité moyenne de défaillance $10^{-3} \leq PFD_{avg}(SIS) = 8{,}5.10^{-3} \leq 10^{-2}$. Cette PFD_{avg} implique, selon la norme (IEC 61511, 2000), un niveau de SIL égal à 2.

Cette évaluation montre que la configuration optimale déterminée par les algorithmes génétiques répond réellement aux exigences du SIL requis par le système d'alimentation en kérosène d'une station de coating de l'entreprise ALGESCO.

Conclusion générale

Nous avons pu à travers ce travail traiter le problème de conception optimale du SIS pour le respect du SIL exigé par le système d'alimentation en kérosène d'une station de coating de l'entreprise ALGESCO.

Nous avons utilisé un AG pour l'optimisation de la structure du SIS et l'obtention de sa configuration optimale pour les SIL exigés sous forme de BdF.

Le problème de conception optimale des SIS a été ramené à un problème de minimisation du coût global du SIS sous contrainte du SIL exigé qui est exprimé en fonction de la fiabilité du SIS.

La conception optimale du SIS a été faite par le choix d'un nombre et types de composants dans chaque sous-système du SIS afin de garantir un coût global minimal et sous contrainte du SIL exigé.

Cette démarche nous a permis d'obtenir par l'AG correspond à celui obtenu par un algorithme déterministe. Le prix du SIS est de 2600$ et son SIL est de niveau 2, ce qui veut dire qu'il satisfait à l'objectif de sureté qu'on lui a assigné.

Les résultats de l'application étudiée montrent son importance pour la conception des systèmes complexes en général et des SIS en particulier.

Réferences bibliographiques

Desroches, A., Leroy, A., & Vallée, F. (2003). *La gestion des risques : principes et pratiques, volume 1.* Edition Lavoisier, France.

Dhillon, B. S., & Yang, N. (1997). Comparisons of block diagram and markov method system reliability and mean time to failure results for constant and non constant unit failure rates. *Microelectronics and Reliability. Vol 37*, 505-509.

Exida. (2005). *Safety related electronic systems for signalling, 2nd edition.* USA.

Goldberg, D. (1994). *Algorithmes génétiques.* Edition Addisson-Wesley, France.

Guo, H., & Yang, X. (2006). A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety. Vol 92*, 1267-1273.

Holland, J. H. (1975). Adaptation In Natural And Artificial Systems. *University of Michigan Press.*

IEC 61061. (1998). *Stratifiés de bois densifiés, non imprégnés, à usage électrique.* Geneva, Switzerland: International Electronical Commission.

IEC 61508. (1998). *Functional of electrical/electronic/programmable electronic (E/E/EP) safety related systems.* Geneva, Switzerland: International Electrotechnical Commission.

IEC 61511. (2000). *Functional safety : Safety instrumented systems for the process industry sector.* Geneva, Switzerland: International Electrotechnical Commission.

ISO/CEI 73. (2002). *Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes.* Geneva, Switzerland: International Standards Organisation.

Kuo, W., Hwang, C. L., & Tillman, F. A. (2001). Optimal reliability design : fundamentals and applications. *Cambridge University Press.*

Li, F., & Aggarwal, R. K. (200). Fast and accurate power dispatch using a relaxed genetic algorithm and a local gradient technique. *Expert Systems with Applications*, 159-165.

Liang, G. S., & Wang, J. J. (1993). Fuzzy fault-tree analysis using failure possibility. *Microelectronics and reliability*, 583-597.

Ludovic, M. (1994). *Audit de sécurité par algorithmes génétiques.* Thèse de doctorat, Université de Rennes 1, France.

Mechri, W. (2011). *Evaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis.* Thèse de doctorat, Ecole Nationale d'Ingénieurs de tunis, Tunisie.

Michalewiez, Z., & Fogel, D. B. (2000). *How to solve it : Modern heuristics.* Springer-Verlag.

OREDA. (2002). *Offshore Reliability. Data Handbook, 4th edition.* Norway.

Ouarzizi, A. E. (1997). Line fitting in noisy data using genetic algorithm. In 3rd international Conference. *Contrôle Qualité par Vision Artificielle QCAV'97*, (pp. 214-217).

Sallak, M. (2008). *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, Institut National Polytechnique de Lorraine, Nancy, France.

VILLEMEUR, A. (1987). *évaluation de la fiabilité, disponibilité et maintenabilité des systèmes réparables : la méthode de l'Espace des Etats.* Edition Eyrolles.

Villemeur, A. (1998). *Sureté de fonctionnement des syst ?mes industriels.* Edition Eyrolls.

Vladimir, F. (2003). Fine-grained tournament selection operator in genetic algorithms. *Computing and Informatics*, 143-162.

Annexes

Annexe 1. Fonctions utilisés sur MATLAB pour l'optimisation avec les AG

1. Fonction objectif

```
function prix = SIS_K(n)
  n=floor(n);
  prix=500*n(1)+500*n(2)+100*n(3)+100*n(4);
end
```

2. Fonction contrainte

```
function [c, ceq] = contrainte_K(n)
  c(1)=-(1-(1-0.9975)^n(1))*(1-(1-0.9975)^n(2))*(1-(1-
    0.9076)^n(3))*(1-(1-0.9806)^n(4))+0.99;
  c(2)=(1-(1-0.9975)^n(1))*(1-(1-0.9975)^n(2))*(1-(1-
  0.9076)^n(3))*(1-(1-0.9806)^n(4))-0.999;
  ceq=[];
end
```

Annexe 2. Calcul flou des PFD_{avg}

Événement de base	Taux de défaillance (/h)			$\widetilde{P(A_i)}$			$PFD_{avg}(A_i)$	%
	low	mean	high	a_i (low)	m_i (mean)	b_i (high)		
Défaillance Capteur de débit	7.10^{-10}	$1{,}758.10^{-7}$	$6{,}679.10^{-7}$	$6{,}136.10^{-6}$	$1{,}5399.10\text{-}^{3}$	$5{,}8377.10^{-3}$	$2{,}4612.10^{-3}$	0,998586
Défaillance unité logique	$3{,}8499.10^{-7}$	$8{,}0607.10^{-6}$	$2{,}6237.10^{-5}$	$3{,}3691.\ 10^{-3}$	$6{,}82214.10^{-2}$	$2{,}0546.10^{-1}$	$9{,}2351.10^{-2}$	$7{,}0925.10^{-4}$
Défaillance Vanne d'isolement automatique	0	$1{,}1628.10^{-6}$	$5{,}6028.10^{-6}$	0	$2{,}01798.10^{-2}$	$9{,}35581.10^{-2}$	$3{,}7467.10^{-4}$	$1{,}6435.10^{-5}$