**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**

# Optimisation d'un Système Instrumenté de Sécurité par les Algorithmes Évolutionnaires.

**Ouail HIMRANE**

| | | |
|---|---|---|
| **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**

# Optimisation d'un Système Instrumenté de Sécurité par les Algorithmes Évolutionnaires.

**Ouail HIMRANE**

| | | |
|---|---|---|
| **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**

# Dédicace

*Je dédie ce travail à :*

*Ma mère et mon père.*

*Mon frère Aimen.*

*Aux membres de ma famille.*

*Mes proches et mes amis.*

*Toute personne qui m'est chère.*

*Tous ceux qui ont cru en moi.*

# Remerciements

*Mes remercîments s'adressent tout d'abord à ALLAH Le Tout Puissant pour la force qu'il m'a donné pour atteindre mes objectifs et arriver où je suis.*

*Mes 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.*

*Je souhaiterais adresser mes vifs remerciements aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire :*

*À Monsieur B. BOUSBAÏ, mon promoteur de l'entreprise, pour m'avoir fait confiance et mis à ma disposition toutes les ressources nécessaires pour l'accomplissement de ma mission. Pour son encadrement, ses remarques ainsi que ses précieux conseils durant toute la période du stage où j'ai pu bénéficier de sa riche expérience et savoir-faire. Pour son accueille, sa bienveillance, sa patience et son savoir-être, qui ont toujours suscités mon 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 j'ai bénéficié.*

*À monsieur B. BENKOUSSAS, professeur à l'ENP, pour ses conseils et sa confiance en m'ont motivé à me surpasser dans la réalisation de ce rapport.*

*Mes remerciements s'adressent également à toute l'équipe de GE Oil & Gas ALGESCO, avec qui, ce fut un plaisir de travailler. 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 ce 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.*

*Ma gratitude se destine également aux enseignants du Département QHSE-GRI de l'Ecole Nationale Polytechnique qui ont contribué à ma formation.*

*À toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce travail, je présente mon respect et ma gratitude.*

**ملخص :** الدافع الرئيسي لهذا العمل هو اقتراح حل لمشكلة الاستجابة للقيود. تنتج هذه المشكلة من خلال البحث عن البنية المثلى لنظام الحماية المجهز الذي يلبي مستوى الموثوقية المطلوب بأدنى تكلفة ممكنة. الجزء الأول يقدم الإطار الرسمي للمشكلة ولمحة عامة عن نماذج مختلفة من أجل حل مشاكل الاستجابة للقيود. أما الجزء الثاني فيعتمد على استخدام الذكاء الاصطناعي، من خلال تطبيق الخوارزميات التطورية للعثور على البنية الأمثل للنظام. في الأخير، دراسة باستعمال سلاسل ماركوف للتحقق من معايير أداء النظام.

**الكلمات الدالة** :الانظمة المجهزة لسلامة ,الخوارزميات التطورية ,سلاسل ماركوف,SIL, تكلفة.

**ABSTRACT :** The main aim of this study is to provide a solution to a constraint satisfaction problem. Such a problem results in searching an optimal architecture of a safety instrumented system that meets a requisite level of reliability, considering minimum costs. In the first part, the study presents a formal framework for the statement of the problem. To solve constraint satisfaction problems, the study sketches/treats an overview of different available models. The second part of the study discusses the exploitation of artificial intelligence using evolutionary algorithm in order to reach the optimal architecture system. A Markov chain study will be verifying the performance parameters of the optimized system.

**Key Words** : SIS, Optimisation, Evolutionary Algorithm, Cost, SIL, Markov

**Résumé :** La motivation principale de ce travail est de proposer une solution à un problème de satisfaction de contraintes. Ce problème de satisfaction de contraintes se traduit par la recherche de l'architecture optimale d'un système instrumenté de sécurité satisfaisant un niveau de fiabilité requis, dans une optique de coûts minimales. La première partie présentera le cadre formel de la problématique, ainsi qu'un tour d'horizon des différents modèles disponibles pour la résolution des problèmes de satisfaction de contraintes. La deuxième partie traitera de l'exploitation de l'intelligence artificielle, par l'application des Algorithmes Évolutionnaires, afin de trouver l'architecture optimale du système. Une étude par chaine de Markov viendra vérifier les paramètres de performance du système optimisé.

**Mots clés** : SIS, Optimisation, Algorithme Évolutionnaire, Coût,, SIL Markov

# Table des matières

# Liste des Tableaux

# Liste des Figures

# Liste des abréviations

| | |
|---|---|
| **BTS** | Barrières Techniques de Sécurité |
| **CSP** | Constraint Satisfaction Problem |
| **COP** | Contrained Optimisation Problem |
| **E/E/EP** | électrique/électronique/électronique programmable |
| **IC** | Intelligence Computationnelle |
| **IEC** | International Electrotechnical Commission |
| **INERIS** | Institut national de l'environnement industriel et des risques |
| **LS** | Logic Solver |
| **MTBF** | Mean Time Between Failures |
| **MTTF** | Mean Time To Failure |
| **MTTR** | Mean Time To Repair |
| **PFD** | Probability of Failure on Demand |
| **PFDavg** | Average Probability of Failure on Demand |
| **PFH** | Probability of a dangerous Failure per Hour |
| **RBDO** | Reliability Based Design Optimization |
| **SdF** | Sûreté de fonctionnement |
| **SIF** | Safety Instrumented Function |
| **S.I.S** | Systèmes Instrumentés de Sécurité |

# Introduction générale

La conception optimale des structures des systèmes soulève depuis des années le plus vif intérêt. Encore trop peu appliquée aux techniques classiques de bureau d'études, elle s'y intègre progressivement au fur et à mesure que s'accroît sa fiabilité. Parti des problèmes les plus simples, le champ d'application de l'optimisation des structures s'étend aujourd'hui à de nouveaux défis toujours plus intéressants.

La simulation numérique dans le domaine du calcul des structures mécaniques a connu de nombreuses évolutions durant ces dernières années grâce au progrès du calcul scientifique, au développement des ordinateurs et à leur croissance tant dans leur vitesse de traitement que dans la qualité d'informations gérées. L'ingénieur dispose donc d'un large éventail de méthodes, supportées par des outils informatiques, notamment la méthode des éléments finis et les méthodes d'optimisation qui constituent des alliés précieux pour la conception optimale des structures dans le respect de certaines règles ou normes

La puissance de calcul des méthodes modernes est le fruit de l'intelligence computationnelle qui est un domaine scientifique lié à l'intelligence artificielle. Parmi les méthodes utilisées dans ce domaine, nous comptons les heuristiques, la logique floue, les réseaux de neurones et les algorithmes évolutionnistes.

La motivation principale de ce mémoire est l'optimisation de l'architecture d'un système est la détermination de la meilleure conception possible en termes de coût et de fiabilité en utilisant une des méthodes basées sur l'intelligence computationnelle.

Pour cela, nous commencerons par une description du contexte général de notre travail, en présentant les principales notions et concepts intervenant dans le domaine de la sûreté de fonctionnement.

Nous présenterons ensuite un aperçu sur méthodes de résolution permettant de répondre à notre problématique. Cela nous permettra de choisir la méthodologie et l'approche à suivre pour atteindre les objectifs de ce travail.

Dans le deuxième chapitre, nous présenterons les algorithmes évolutionnaires que nous utiliserons comme outil pour l'optimisation de l'architecture de notre système.

Le troisième chapitre sera consacré à l'application des méthodes évolutionnaires à un Systèmes Instrumentés de Sécurité dans le cadre de la résolution d'un problème d'optimisation sous contraintes.

Dans le dernier, nous utiliserons l'approche Markovienne afin de valider l'architecture du système optimisée.

# Chapitre 1.
# Contexte générale
# et problématique

# Chapitre 1. Contexte général et problématique

## 1.1. Introduction

Dans ce premier chapitre, nous commencerons par une description du contexte général de notre travail, en présentant les principales notions et concepts intervenant dans le domaine de la sûreté de fonctionnement.

Nous nous intéresserons particulièrement aux Systèmes Instrumentés de Sécurité SIS qui constituent an axe important du domaine de la sécurité des biens et des personnes.

Nous exposerons ensuite la problématique que nous essaierons de résoudre afin de bien définir les objectifs de ce travail.

Enfin, un aperçu sur méthodes de résolution permettant de répondre à notre problématique, nous permettra de choisir la méthodologie et l'approche à suivre pour atteindre les objectifs de ce travail.

## 1.2. Principaux concepts de la SdF

### 1.2.1. Sûreté de fonctionnement

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 Sûreté de fonctionnement (SdF) est considérée comme la science des défaillances et des pannes.

### 1.2.2. 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.

### 1.2.3. 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, 2014).

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).

### 1.2.4. 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.*

### 1.2.5. Barrières Techniques de Sécurité (BTS)

Les barrières de sécurité (ou mesures de maîtrise des risques) sont de trois types :

- Les barrières techniques ;

- Les barrières humaines ;
- Les barrières qui font intervenir les barrières techniques et humaines. Ces barrières sont appelées systèmes à action manuelle de sécurité.

Dans la catégorie des barrières techniques de sécurité, on trouve les dispositifs de sécurité ou les systèmes instrumentés de sécurité. Le schéma suivant résume toutes les BTS étudiées dans la littérature :

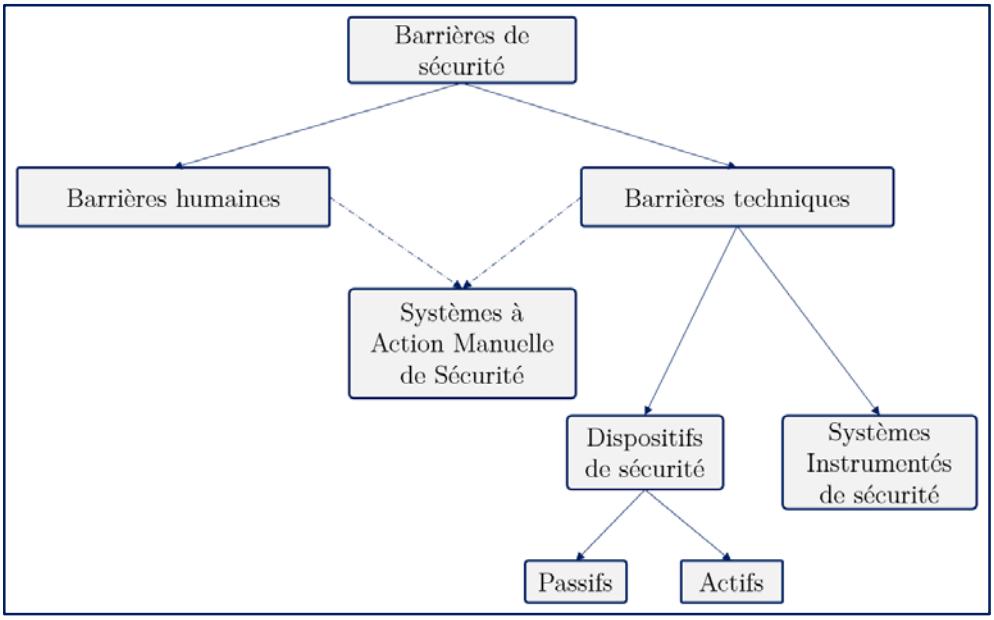


*Figure 1-1 : Types de BTS.*

### 1.2.6. Dispositifs de sécurité

Un dispositif de sécurité est en général un élément unitaire, autonome, ayant pour objectif de remplir une fonction de sécurité, dans sa globalité. Un dispositif peut être classé en 2 catégories :

- Dispositif de sécurité passive ;
- Dispositif de sécurité active.

#### 1.2.6.1. Dispositif de sécurité passive

La sécurité passive désigne tous les éléments mis en jeu afin de réduire les conséquences d'un accident lorsque celui-ci n'a pu être évité. Elle agit par sa seule présence, elle ne met en jeu aucun système mécanique pour remplir sa fonction et ne nécessite ni action humaine (hors intervention de type maintenance), ni action d'une mesure technique, ni source d'énergie externe pour remplir sa fonction.

On retrouve notamment dans cette catégorie les cuvettes de rétention, les disques de rupture, les arrête-flammes ainsi que les murs coupe-feu.

Cependant, il ne faut pas réduire la sécurité passive à la limitation des conséquences des accidents (l'isolation électrique est une mesure passive et préventive).

#### 1.2.6.2. Dispositif de sécurité active

La sécurité active désigne tous les éléments mis en jeu afin d'éviter les accidents. Elle nécessite une action, une énergie et un entretien. Elle met en jeu des dispositifs mécaniques (ressort, levier…) pour remplir sa fonction.

On retrouve notamment dans cette catégorie les soupapes de décharge et les clapets limiteurs de débit. Ils peuvent nécessiter une source d'énergie externe pour fonctionner.

Notons qu'une vanne de sécurité n'est pas considérée comme un dispositif de sécurité, car elle n'assure pas à elle seule une fonction de sécurité dans sa globalité. Il faut une action humaine et/ou une source d'énergie externe pour l'actionner.

La sécurité d'une installation repose sur l'utilisation de ces deux modes d'action. Une préférence est donnée au mode passif quand il est techniquement possible. Des critères de qualité sont exigés pour le mode actif, notamment la tolérance à la première défaillance.

La sécurité fonctionnelle reste l'un des moyens les plus importants pour la prise en compte des risques. D'autres moyens de réduction ou d'élimination des risques, tels que la sécurité intégrée dans la conception, sont également d'une importance essentielle.

## 1.3. Paramètres de performances en Sûreté de fonctionnement

### 1.3.1. 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.

### 1.3.2. Maintenabilité M(t)

Aptitude d'une entité à être remise en état, par une maintenance donnée, d'accomplir des fonctions requises dans les conditions données.

Elle se caractérise par la probabilité M(t) d'être en état, à l'instant t, d'accomplir ces fonctions sachant qu'elle était en panne à l'instant 0.

### 1.3.3. Disponibilité A(t)

Aptitude d'une entité à être en état d'accomplir les fonctions requises dans les conditions données.

Elle se caractérise par la probabilité A(t) d'être en état, à l'instant t, de bon fonctionnement et d'accomplir les fonctions requises.

À l'opposé de la fiabilité, la disponibilité s'intéresse à la probabilité que le système fonctionne à un instant donné sans se préoccuper de ce qui s'est passé auparavant. Elle caractérise donc un fonctionnement pouvant être interrompu puis repris.

### 1.3.4. Indisponibilité et Défiabilité

Les probabilités complémentaires D (t) et U (t) de la fiabilité et de la disponibilité sont dénommées « défiabilité » et « indisponibilité » :

$$D\,(t) = 1 - R\,(t) \tag{1.1}$$

$$U\,(t) = 1 - A\,(t) \tag{1.2}$$

### 1.3.5. Taux de défaillance

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

$$\lambda(t) = \frac{-dR(t)/dt}{R(t)} \tag{1.3}$$

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.

### 1.3.6. Taux de réparation

Le taux de réparation, généralement noté $\mu(t)$, est :

$$\mu(t) = \frac{-dM(t)/dt}{M(t)} \quad 1.4$$

Si on le suppose constant :

$$M(t) = e^{-\mu t} \quad 1.5$$

### 1.3.7. MTBF (Mean Time Between Failures)

Moyenne des temps de bon fonctionnement ou MTBF est la moyenne des temps séparant deux défaillances consécutives.

Dans le cas très usuel où l'hypothèse du taux de défaillance constant est retenue :

$$MTBF = \frac{1}{\lambda} \quad 1.6$$

### 1.3.8. MTTF (Mean Time To Failure)

Le MTTF est la moyenne des durées de fonctionnement de l'instant 0 à la première défaillance. C'est donc le temps moyen avant la première défaillance.

Il est à noter que, pour un composant élémentaire régi par une loi exponentielle de taux de défaillance $\lambda$ :

$$MTTF \approx MTBF = \frac{1}{\lambda} \quad 1.7$$

### 1.3.9. MTTR (Mean Time To Repair)

C'est la moyenne sur un ensemble d'entités « identiques » et sur l'ensemble des cycles défaillance / réparation de la durée de vie considérée des TTR

$$MTBF = MUT + MTTR \quad 1.8$$

## 1.4. 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 »:

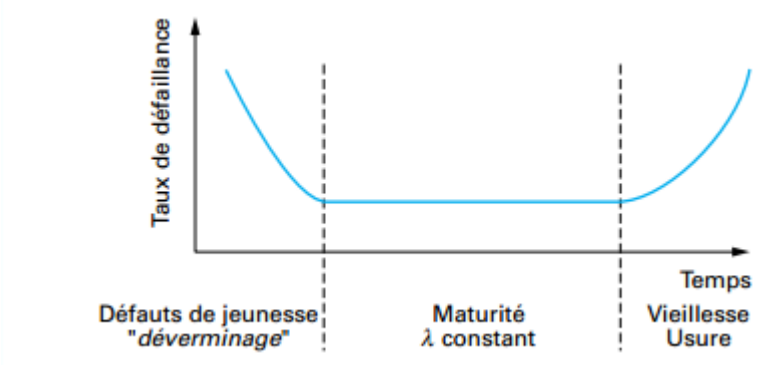


*Figure 1-2 : Courbe en baignoire.*

- 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 :

$$R(t) = e^{-\lambda t} \qquad 1.9$$

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

## 1.5. 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.*

### 1.5.1. 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.*

#### 1.5.1.1. 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.

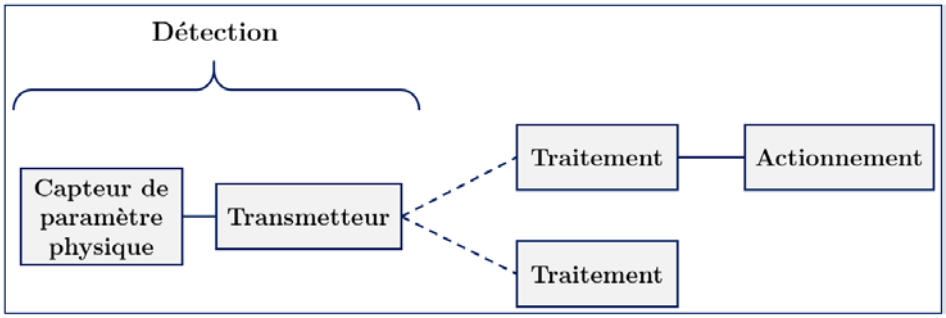


*Figure 1-4. Architecture depuis le capteur jusqu'à l'actionneur (INERIS, 2008)*

#### 1.5.1.2. 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.

#### 1.5.1.3. 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.

### 1.5.2. 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).

### 1.5.3. 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).

#### 1.5.3.1. 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 relatif à la sécurité, qui rend ce dernier incapable d'effectuer correctement sa fonction de sécurité, lorsqu'il est faiblement sollicité.

#### 1.5.3.2. 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.

## 1.6. Problématique

### 1.6.1. Redondance au sein d'un S.I.S.

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.

Nous pouvons distinguer plusieurs types de redondance :

**la redondance active** qui est une redondance telle que tous les moyens d'accomplir une fonction requise fonctionnent simultanément.

**la redondance 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.

**la 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.

### 1.6.2. Notion d'optimisation

L'optimisation de l'architecture d'un système a pour objectif la détermination de la meilleure conception possible en termes de coût et de qualité. En général, le concepteur considère un critère d'optimisation, des restrictions et des variables de conception de type numérique et fait appel à des procédures de type déterministe. En réponse à ces difficultés, des méthodes d'analyse intègrent le caractère aléatoire. Une première démarche a été le contrôle du niveau de fiabilité. Ainsi, il est usuel de chercher à déterminer une conception optimale satisfaisant un niveau minimal de fiabilité.

### 1.6.3. Objectif

L'objectif de notre travail est de proposer une solution à un problème de satisfaction de contraintes (CSP) constitué d'un ensemble de variables dont les valeurs sont issues d'un ensemble de valeurs appelé domaine, et dont l'affectation est soumise à certaines conditions appelées contraintes.

Ce problème de satisfaction de contraintes se traduit par la recherche de conception optimale d'un système instrumenté de sécurité satisfaisant un niveau minimal de fiabilité dans l'optique de coûts minimales.

## 1.7. Conclusion

La connaissance des notions importantes intervenant dans la sûreté de fonctionnement des équipements nous a permis d'avoir une vision claire sur la démarche à suivre pour répondre aux objectifs fixés par la problématique,

L'optimisation de l'architecture de notre système a pour objectif la détermination de la meilleure conception possible en termes de coût et de qualité en contrôlant le niveau de fiabilité. L'objectif de cette optimisation fiabiliste (RBDO, Reliability Based Design Optimization) est de trouver la solution optimale qui vérifie une probabilité de défaillance inférieure ou égale à la probabilité cible.

Il existe de très nombreuses méthodes de résolution pour les problèmes d'optimisation. De nombreuses classifications de ces méthodes ont été proposées dans la littérature : méthodes complètes et incomplètes, méthodes issues de la recherche opérationnelle et méthodes issues de l'intelligence artificielle.

La méthodologie de travail que nous adoptons pour la résolution de notre problématique suivra une approche basée sur l'intelligence computationnelle qui est un domaine scientifique lié à l'intelligence artificielle. De ce fait, les algorithmes évolutionnistes, comptant parmi les méthodes utilisées dans ce domaine, constituent l'outil principale de la démarche de résolution de notre problématique et feront l'objet du prochain chapitre.

# Chapitre 2. Démarche d'optimisation par algorithmes évolutionnaires

# Chapitre 2. Démarche d'optimisation par Algorithmes évolutionnaires

## 2.1. Introduction

Le 24 novembre 1859, Charles Darwin publie un ouvrage scientifique nommé « L'origine des espèces ». Cet ouvrage sera considéré par la suite comme le texte fondateur de la théorie de l'évolution. Dans ce livre, Darwin présente la théorie scientifique de l'évolution des espèces vivantes à partir d'autres espèces généralement éteintes, au moyen de la sélection naturelle. Darwin avance un ensemble de preuves montrant que les espèces n'ont pas été créées indépendamment et ne sont pas immuables.

Les algorithmes évolutionnistes ou algorithmes évolutionnaires (evolutionary computation en anglais), sont une famille d'algorithmes dont le principe s'inspire de la théorie de l'évolution pour résoudre des problèmes divers. Ce sont donc des méthodes de calcul bioinspirés. L'idée est de faire évoluer un ensemble de solutions à un problème donné, dans l'optique de trouver les meilleurs résultats. Ce sont des algorithmes dits stochastiques, car ils utilisent itérativement des processus aléatoires.

La grande majorité de ces méthodes sont utilisées pour résoudre des problèmes d'optimisation, elles sont en cela des métaheuristiques. On les classe également parmi les méthodes d'intelligence computationnelle.

Une métaheuristique est un algorithme d'optimisation visant à résoudre des problèmes d'optimisation difficile (souvent issus des domaines de la recherche opérationnelle, de l'ingénierie ou de l'intelligence artificielle) pour lesquels on ne connaît pas de méthode classique plus efficace.

Dans ce chapitre, nous présenterons les algorithmes évolutionnaires que nous utiliserons dans la suite de ce document comme un outil pour l'optimisation de l'architecture du SIS.

## 2.2. Principe de base des algorithmes évolutionnaires

Les algorithmes évolutionnaires se basent sur l'observation des phénomènes biologiques mis en œuvre par des populations d'organismes vivants en vue de s'adapter à leur environnement. Ces mécanismes de sélection et d'héritage génétique représentent une version artificielle de la théorie de l'évolution selon Darwin. Cette discipline couvre ainsi un ensemble de techniques, nommées « algorithmes génétiques », « programmation

génétique », « stratégies d'évolution », « programmation évolutionnaire ». Le domaine des algorithmes évolutionnaires est en pleine expansion tant au niveau théorique qu'au niveau applicatif.

Les principes de base des algorithmes évolutionnaires (AE) 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. En d'autres termes, ces algorithmes évolutionnaires représentent une version artificielle, informatique, de la théorie de l'évolution selon Darwin.

Depuis une quarantaine d'années, de nombreuses méthodes de résolution de problèmes, d'optimisation stochastique, ont été développées à partir de ces principes simplifiés à l'extrême pour les besoins informatiques. C'est ce que l'on commence actuellement à nommer de façon générale le « darwinisme artificiel ». Le terme « algorithmes évolutionnaires » couvre ainsi un ensemble de techniques, nommées « algorithmes génétiques », « programmation génétique », « stratégies d'évolution », « programmation évolutionnaire », suivant la façon dont les principes darwiniens sont traduits dans le modèle artificiel.

## 2.3. Darwinisme, évolutionnisme

Le darwinisme désigne, en son sens strict, la théorie, formulée en 1859 (dans De l'origine des espèces) par le naturaliste anglais Charles Darwin, et qui explique « l'évolution biologique des espèces par la sélection naturelle et la concurrence vitale » (Dictionnaire de l'Académie française, 9e édition)

C'est par l'observation patiente et systématique des lignées d'espèces, que Charles Darwin a construit sa théorie de l'évolution des espèces.

Selon lui, l'évolution se fonde sur trois principes (extrait de La Grande Encyclopédie Larousse, 1973) :

— partout, toujours, et de mille manières, les faunes et les flores ont varié ;

— les lignées observées individuellement par voie d'élevage ou de culture, présentent d'innombrables variations de détail ;

— la lutte pour la vie est si féroce et la sélection naturelle si rigoureuse que la moindre variation utile fait triompher la lignée qui la possède.

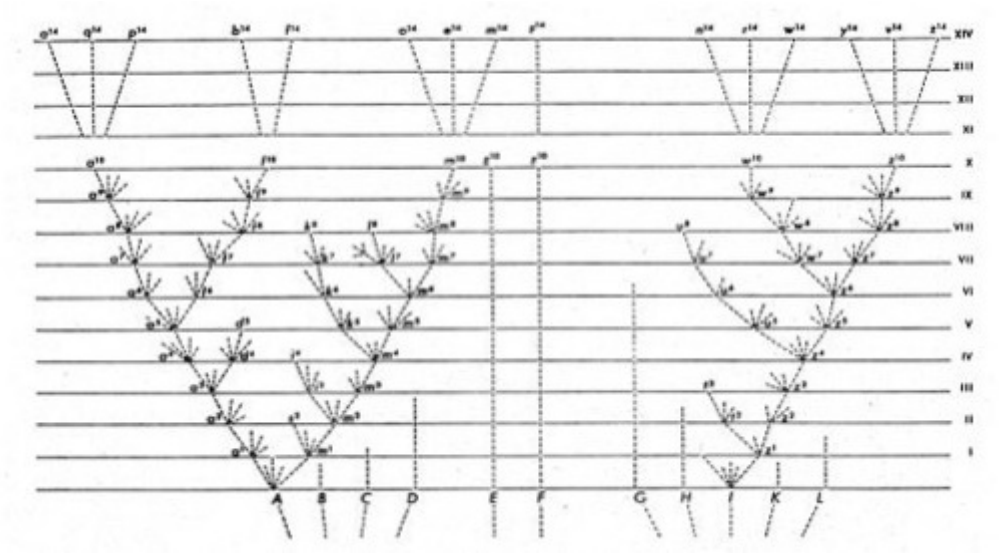


*Figure 2-1 : L'« arbre de la vie », tel que le représente Charles Darwin dans son ouvrage L'Origine des espèces, où il présente ses théories sur l'évolution des êtres vivants (Davis, 1987)*

Selon la théorie de l'évolution, plusieurs mécanismes sont à l'œuvre pour ce faire. Schématiquement :

- Les caractéristiques d'un organisme sont en grande partie codées dans ses gènes,
- chaque population d'organismes est composée d'individus tous différents,
- les individus sont plus ou moins adapté à leur environnement,
- les organismes transmettent une partie de leurs caractéristiques à leurs descendants,
- les individus les plus adaptés se reproduisent plus « efficacement », leurs caractéristiques ont donc tendance à davantage se répandre dans la population.

## 2.4. Bref historique du domaine artificiel du darwinisme

L'idée d'utiliser les principes des processus d'évolution organique en tant que technique d'optimisation globale a émergé indépendamment des deux côtés de l'océan Atlantique il y a une quarantaine d'années.

Ces deux approches reposent, comme nous l'avons dit, sur l'imitation du phénomène d'apprentissage collectif – on dit aussi d'adaptation – d'une population naturelle, fondée sur les observations de Darwin et sur la théorie moderne de l'évolution.

Le courant américain, initialisé par Holland dans les années soixante, est à l'origine de ce que l'on appelle les Algorithmes Génétiques (AG) (HOLLAND, 1975). Bien qu'ils aient été prévus initialement dans le cadre d'optimisation ou d'adaptations dans le domaine

discret, les AG ont été facilement étendus à l'optimisation sur des domaines continus (DE JONG, 1975).

En Allemagne, sont apparues à peu près en même temps des méthodes appelées Stratégies d'Évolution (SE) ( (RECHENBERG, 1973) puis (SCHWEFEL, 1975) voir (HOFFMEISTER & BAECK, 1992)). Ces méthodes étaient au contraire prévues initialement pour fonctionner sur des domaines continus, et ont été étendues à des applications en optimisation discrète.

D'autres approches, plus récentes, comme les algorithmes à estimation de distributions, correspondent à une interprétation plus statistique et plus globale des opérateurs génétiques (travaux de (MUHLENBEIN & PAASS, 1996), (GOLDBERG & PELIKAN, 2002), (LARRANAGA & LOZANO, 2002)).

## 2.5. Démarche des Algorithmes Évolutionnaires

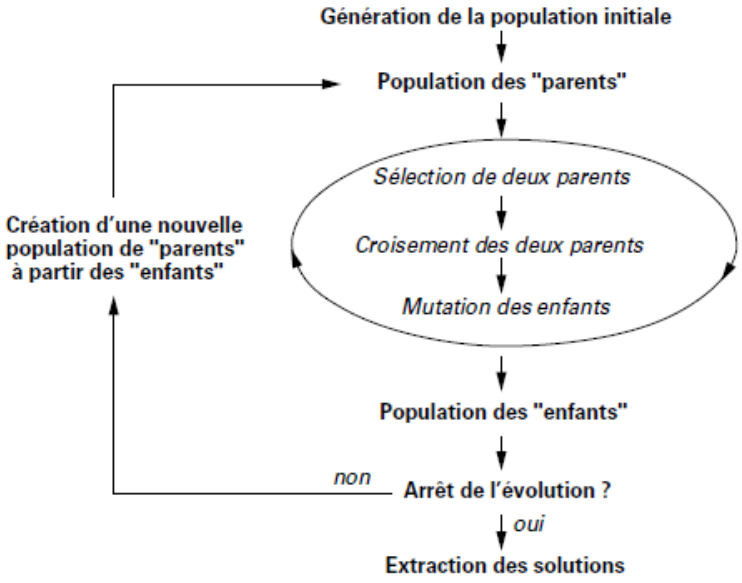


*Figure 2-2 : Organigramme de l'algorithme évolutionnaire simple. (LUTTON, 2006)*

La base d'un algorithme évolutionnaire classique est une boucle générationnelle de populations d'individus (représentés sous forme discrète ou continue, à l'aide de chromosomes ou gènes) correspondant chacun à une solution au problème considéré (voir (Davis, 1987) (GOLDBERG D. , 1989) (MICHALEWICZ, 1996)). Cela mène au schéma de la figure 2.2, dont les étapes principales sont les suivantes.

• **La sélection,** pour détecter quels individus de la population courante seront autorisés à se reproduire (les parents). Cette opération est fondée sur la qualité des individus,

estimée à l'aide d'une fonction, nommée fitness, fonction d'évaluation, ou encore performance.

Le paramètre principal de cette étape de sélection est ce que l'on appelle la pression sélective, qui correspond globalement au quotient de la probabilité de sélection du meilleur individu sur la probabilité de sélection de l'individu moyen de la population courante. Ce paramètre gère la rapidité de concentration de la population autour de son meilleur individu.

• **La reproduction**, où les parents sélectionnés sont utilisés pour générer des descendants. Les deux opérations principales sont le croisement, qui combine les gènes de deux parents, et la mutation qui consiste en une légère perturbation du génome. Ces opérations sont appliquées aléatoirement, et dépendent de deux paramètres, la probabilité de croisement pc et la probabilité de mutation pm. Ces probabilités sont des paramètres très importants, qui influent de façon considérable sur la qualité des résultats globaux (convergence et qualité des résultats).

• **L'évaluation,** qui consiste à calculer (ou estimer) la qualité des individus nouvellement créés. C'est là, et uniquement là qu'intervient la fonction à optimiser. Aucune hypothèse n'est faite sur la fonction elle-même, excepté le fait qu'elle puisse servir de base au processus de sélection (elle doit pouvoir permettre de définir une probabilité ou au minimum un ordonnancement des solutions).

• **Le remplacement,** enfin, qui gère la manière dont on constitue la génération n + 1. La stratégie simpliste qui consiste à remplacer l'ensemble des parents par tous leurs descendants a été expérimentalement et théoriquement déboutée dans le cadre des applications d'optimisation. Il est nécessaire de maintenir un certain taux d'élitisme[1], tout simplement pour ne pas perdre la mémoire des bons individus visités. Les stratégies usuelles de remplacement consistent à maintenir un pourcentage donné des meilleurs individus de la population courante dans la population suivante ( (DE JONG, 1975) par exemple, emploie un paramètre qui gère le taux de renouvellement de la population, le generation gap ). Ce paramètre est lui aussi essentiel pour le bon comportement de convergence de l'algorithme évolutionnaire.

[1] Élitisme : formation ou à sélection d'une élite au détriment des autres membres du group.

## 2.6. Notions et vocabulaire de base

L'algorithme évolutionnaire fait évoluer sa population de façon à adapter les individus à l'environnement, cela se traduit au sens algorithmique du terme par une maximisation de la fonction d'évaluation sur les individus de la population

Le tableau suivant présentera une analogie du vocabulaire des AE avec la biologie

*Tableau 2-1 :* Vocabulaire des AG : une prudente analogie avec la biologie.

| Algorithme évolutionnaire | Méthode d'optimisation |
|---|---|
| Individu | Solution : vecteur |
| Population | Ensemble de solutions |
| Chromosome | Représentation/codage de la solution |
| Croisement ou recombinaison | Opération sur deux codes |
| Mutation | Opération sur un code |
| Environnement | Espace de recherche |
| « Fitness », degré d'adaptation à l'environnement | Valeur de la fonction d'évaluation |
| Évolution | Maximisation de la fonction d'évaluation |

## 2.7. Caractéristiques principales des algorithmes évolutionnaires

La caractéristique principale de ces algorithmes est qu'ils manipulent des populations de solutions et les font évoluer via des opérations stochastiques. Ces opérations sont usuellement organisées en générations et copient de façon très simplifiée la génétique naturelle. Elles sont de deux types :

- **La sélection**, fondée sur la performance d'un individu, ou plus précisément sur une mesure de la qualité de cet individu vis-à-vis du problème que l'on cherche à résoudre ;
- **Les opérateurs génétiques**, le plus souvent nommés croisement et mutation, pour faire un parallèle avec la génétique, et qui produisent de nouveaux individus, pour la génération suivante.

La réussite d'un tel algorithme est fondé sur l'hypothèse que l'action des opérateurs génétiques sur des individus sélectionnés produit statistiquement des individus de plus en plus proches de la solution recherchée. En d'autres termes, le processus stochastique sous-jacent ainsi produit doit être correctement calibré et paramétré pour que les

populations successives convergent vers ce que l'on souhaite, c'est-à-dire le plus souvent l'optimum global de la fonction de performance.

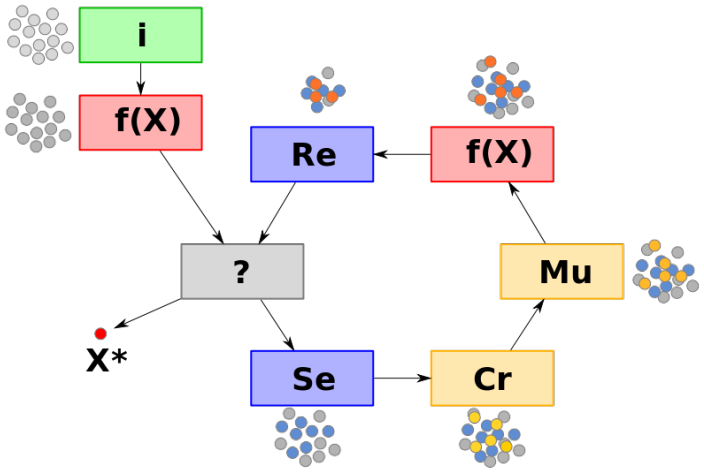


*Figure 2-3 : Les opérateurs de sélections (en bleu) et de variation (en jaune) itératives utilisées dans les algorithmes évolutionnaires.*

Avec :

| | |
|---|---|
| $i$ | Initialisation. |
| $f(X)$ | Évaluation. |
| ? | Critère d'arrêt. |
| $Se$ | Sélection. |
| $Cr$ | Croisement. |
| $Mu$ | Mutation. |
| $Re$ | Remplacement. |
| $X^*$ | Optimum. |

Pour que le système fonctionne correctement, il est en outre nécessaire de gérer :

- **L'initialisation** du processus, qui est usuellement faite de façon Aléatoire
- L'**arrêt** du processus, de même, est essentiel du point de vue pratique. Si l'on a peu ou pas d'informations sur la valeur-cible de l'optimum recherché (ce qui autorise un arrêt dès que cette valeur est atteinte par le meilleur individu de la population courante).

## 2.8. Description du SIS à optimiser

Le SIS que nous proposons d'optimiser intervient lors de de le détection d'une concentration jugée importante d'hydrogène dans l'air.

Il permet de traduire les valeurs détectées en détection en une information recevable par une unité de traitement qui à son tour coupera l'alimentation à la source, en actionnant la fermeture d'une électrovanne.

Ce SIS est composé de trois sous fonctions :

### 2.8.1. Détection :

L'ensemble des détecteurs d'hydrogène $H_2$ mesure la teneur de l'air ambiant en Hydrogène.

Cette valeur de concentration, mesurée en fraction volumique dans l'air, sera transmise sous forme d'un signal électrique à l'unité de traitement logique.

### 2.8.2. Traitement :

L'unité de traitement logique traite les différents signaux, qui lui sont émis par l'ensemble des détecteurs, afin d'en faire ressortir des informations sur la concentration de l'hydrogène dans l'air. L'interprétions de ces données en les comparant aux seuils de concentration tolérables, commandera l'actionnement des « vannes d'isolement automatiques ».

### 2.8.3. Actionnement :

Le système d'actionnent, composé par les « vannes d'isolement automatiques », agit directement sur le système pour neutraliser sa dérive, en coupant l'alimentation en hydrogène à la source par la fermeture des électrovannes permettant l'isolement de l'amené en combustible (générateur d'hydrogène / bouteilles de stockage d'hydrogène)

## 2.9. Diagramme de fiabilité

La méthode des blocs diagrammes de fiabilité est l'une des premières méthodes à avoir été utilisée pour analyser les systèmes et permettre des calculs de fiabilité

(KLEINERMAN & WEISS, 1954). 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.

Elle permet une analyse quantitative qui a pour objectif en particulier de définir la probabilité de bon fonctionnement d'un système. Les calculs reposent sur les probabilités de réussite des missions des éléments constituants le système. Cette méthode est utilisée dans l'évaluation des performances des BTS par le calcul de la $PFD_{avg}$ résultante et la détermination de son niveau de confiance

Ci-après, les représentations de la logique de fonctionnement les plus utilisés ainsi que le calcul de leur fiabilité.

### 2.9.1. Diagramme série

Le diagramme de fiabilité série (figure 2.4) représente un système caractérisé par un enchaînement linéaire de $n$ éléments. La défaillance de l'un des $n$ composants entraînera la défaillance du système complet (Cocozza-Thivent, 1997). La fiabilité du système complet $R_s$ est égale au produit des fiabilités de chaque composant, comme le montre l'équation 3.1:

$$R_s = \prod_{i=1}^{n} R_i \qquad 2.1$$

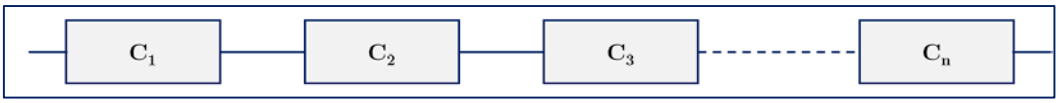


*Figure 2-4 : Représentation d'un diagramme série.*

### 2.9.2. Diagramme parallèle

Le diagramme de fiabilité parallèle (figure 2.5) représente un système caractérisé par une association parallèle de tous les composants. C'est la défaillance de tous les composants qui entrainera la défaillance du système. La fiabilité du système $R_s$ est représenté par l'équation 2.2 :

$$R_s = 1 - \prod_{i=1}^{n} (1 - R_i) \qquad 2.2$$

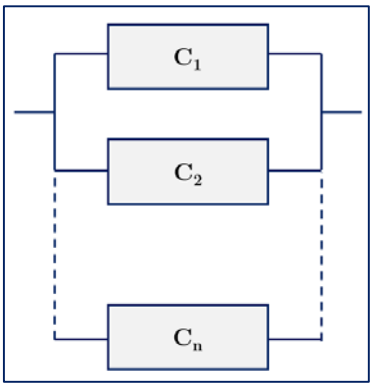


*Figure 2-5. Représentation d'un diagramme parallèle*

### 2.9.3. Diagramme série-parallèle

Le diagramme de fiabilité série-parallèle (figure 2.6) représente un système qui est constitué de $n$ sous-systèmes connectés en parallèle, tel que chaque sous-système est composé de $k$ éléments placés en série. Pour le calcul de la fiabilité, chaque sous-système en série est modélisé par un seul composant, tel que la fiabilité d'un sous-système en série $i$ est égale à :

$$R_i = \prod_{j=1}^{n} R_{ij} \tag{2.3}$$

La fiabilité du système $R_s$ est alors :

$$R_s = 1 - \prod_{i=1}^{n} (1 - R_i) \tag{2.4}$$

Impliquant ainsi :

$$R_s = 1 - \prod_{i=1}^{n} (1 - \prod_{i=1}^{n} R_{ij}) \tag{2.5}$$

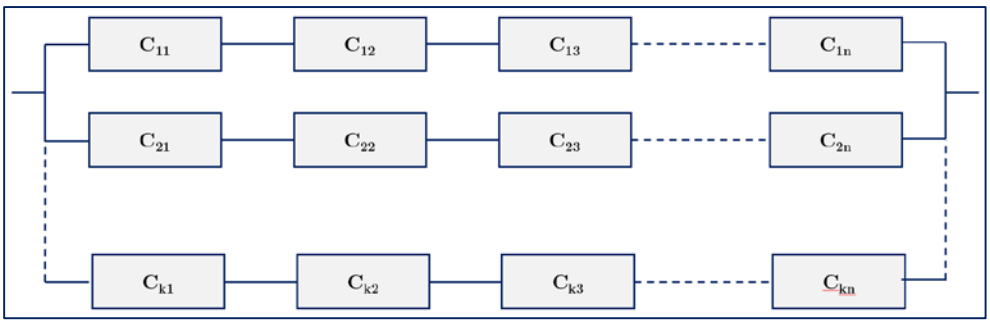


*Figure 2-6. Représentation du diagramme Série-Parallèle*

### 2.9.4. Diagramme parallèle-série

Le diagramme de fiabilité parallèle-série (figure 2.7) représente un système constitué de $n$ sous-système connectés en série, tel que chaque sous-système est composé de $k$ éléments placés en parallèle (Cocozza-Thivent, 1997). Le calcul de la fiabilité se fait en réduisant le système complet en un système série tel que chaque sous système en parallèle est modélisé par un seul composant.

La fiabilité d'un sous-système en parallèle $j$ est égale à :

$$R_j = 1 - \prod_{i=1}^{n}(1 - R_{ij}) \tag{2.6}$$

La fiabilité du système $R_s$ est alors :

$$R_s = \prod_{j=1}^{n} R_{ij} \tag{2.7}$$

Impliquant ainsi :

$$R_s = \prod_{j=1}^{n}\left[1 - \prod_{i=1}^{n}(1 - R_{ij})\right] \tag{2.8}$$

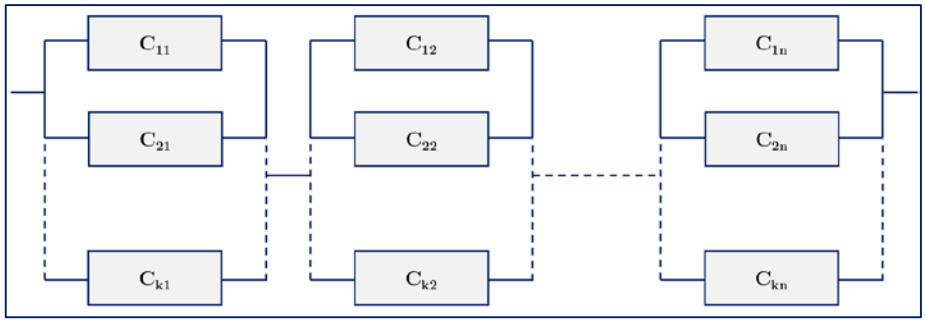


*Figure 2-7. Représentation diagramme Parallèle-Série*

## 2.10. Conclusion

Les algorithmes évolutionnaires s'inspirent de l'évolution des êtres vivants, en considérant que celle-ci tend à produire des organismes plus adaptés à leur environnement.

Après avoir initialisé une première population d'individus, on itère un nombre fini de fois, jusqu'à atteindre un critère d'arrêt (par exemple un nombre maximum de générations). La première étape de sélection permet de séparer les individus qui participeront à la reproduction de ceux qui n'y participeront pas. Les individus sélectionnés (les « parents ») se reproduisent (on dit aussi que l'on effectue des croisements), donnant un ensemble d'« enfants » partageant une partie des caractéristiques de leurs ascendants. Ces enfants subissent alors une étape de mutation, qui modifie aléatoirement leur génotype. Les nouveaux individus sont alors évalués (on met à jour leur valeur en faisant appel à la fonction objectif). Enfin, on choisit un nombre d'individus déterminé parmi l'ensemble parents + enfants, pour former la génération suivante.

Les algorithmes évolutionnaires seront utilisés dans le prochain chapitre comme outil d'intelligence computationnelle exploitant l'intelligence artificielle afin de trouver l'architecture optimale du SIS.

# Chapitre 3. Résultats de l'optimisation du SIS par algorithmes évolutionnaires

# Chapitre 3. Résultat de l'optimisation du SIS par les Algorithmes Évolutionnaires.

## 3.1. Introduction

Pour améliorer le niveau de confiance d'une barrière de sécurité, il est possible, entre autres, de la doubler totalement ou de doubler une partie de ses composants (redondance totale ou partielle de la barrière de sécurité).

L'optimisation de l'architecture d'un système a pour objectif la détermination de la conception optimale, d'une barrière de sécurité, satisfaisant un niveau minimal de fiabilité.

Ce chapitre est consacré à l'application des méthodes évolutionnaires à un Système Instrumenté de Sécurité dans le cadre de la résolution d'un problème d'optimisation sous contraintes. Le but, est de trouver la meilleure solution qui satisfasse toutes les contraintes, dans l'optique de minimiser les coûts

Nous définirons dans un premier temps les contraintes auxquelles doit répondre notre Systèmes Instrumentés de Sécurité. Nous nous intéresserons ensuite au critère d'optimisation que nous essaierons de minimiser, en l'occurrence le coût, afin de trouver la meilleure conception possible en termes de coût et de qualité.

## 3.2. Niveau d'intégrité de sécurité (SIL) requis

La mise en place d'un système instrumenté de sécurité nécessite la détermination du niveau d'intégrité de sécurité (SIL) de cette dernière.

Les normes de sécurité fonctionnelle IEC 61508 et IEC 61511 définissent une démarche d'analyse du niveau d'intégrité de sécurité (SIL) d'un système. Elles permettent de définir le niveau SIL qui doit être atteint par un SIS qui réalise la fonction de sécurité suite à une analyse de risque (Sallak, 2008). Plus le SIL a une valeur élevée plus la réduction du risque est importante.

Les SIS sont classés en quatre niveaux SIL qui se caractérisent par des indicateurs discrets positionnés sur une échelle de un à quatre niveaux (voir Tableau 6.5.1). Les SIL sont employés pour spécifier les exigences de sécurité des fonctions de sécurité réalisées par des systèmes E/E/EP relatifs à la sécurité selon la norme (IEC 61508, 1998). Le SIL "quatre" désigne le degré de sécurité le plus élevé du fait de l'exigence forte de sécurité imposée et le niveau SIL "un" désigne l'exigence la plus faible.

*Tableau 3.1. Différents niveaux de SIL définis par la norme* (IEC 61508, 1998)

| Sollicitation SIL | Demande Faible $PFD_{avg}$ | Demande élevée $PFH$ |
|---|---|---|
| 1 | $[10^{-2}; 10^{-1}]$ | $[10^{-6}; 10^{-5}]$ |
| 2 | $[10^{-3}; 10^{-2}]$ | $[10^{-7}; 10^{-6}]$ |
| 3 | $[10^{-4}; 10^{-3}]$ | $[10^{-8}; 10^{-7}]$ |
| 4 | $[10^{-5}; 10^{-4}]$ | $[10^{-9}; 10^{-8}]$ |

L'utilisation des niveaux SIL permet de prendre en compte les défaillances rares mais possibles des systèmes de sécurité en plus des défaillances inhérentes au système opérationnel, menant aux événements dangereux identifiés pendant l'analyse de risque. Les SIL sont attribués aux fonctions de sécurité sur la base de l'étude des défaillances (IEC 61508, 1998).

Le SIL requis pour le SIS que nous proposons d'optimiser est évalué au niveau trois.

## 3.3. Paramètres du SIS à optimiser

La base de données (OREDA, 2002) donne les valeurs les taux de défaillance de chaque composant du système

*Tableau 3-1 : les taux de défaillance de chaque composant du système.*

| | $\lambda_{Low}$ | $\lambda_{\text{Medium}}$ | $\lambda_{\text{High}}$ |
|---|---|---|---|
| Détecteur d'hydrogène | $7{,}99733.10^{-08}$ | $3{,}70347.10^{-07}$ | $8{,}22396.10^{-07}$ |
| Unité de traitement logique | $3{,}84986.10^{-07}$ | $8{,}06066.10^{-06}$ | $2{,}62371.10^{-05}$ |
| Vanne d'isolement automatique | 0 | $1{,}1628.10^{-06}$ | $5{,}6028.10^{-06}$ |

Le temps considéré pour notre étude est 1 an = 8766 h

$$R(t) = e^{-\lambda.t} \tag{3.1}$$

$$R = \frac{R_{Low} + R_{\text{Medium}} + R_{\text{High}}}{3} \tag{3.2}$$

*Tableau 3-2 : Fiabilité des composants du SIS*

| | $R_{Low}$ | $R_{Medium}$ | $R_{High}$ | **R** |
|---|---|---|---|---|
| Détecteur d'hydrogène | 0,9992992 | 0,9967588 | 0,9928168 | **0,9962916** |
| Unité de traitement logique | 0,9966309 | 0,93177887 | 0,7945377 | **0,907649157** |
| Vanne d'isolement automatique | 1 | 0,989858669 | 0,952072449 | **0,980643706** |

$$PFD = 1 - R \tag{3.3}$$

*Tableau 3-3 : Probabilité de défaillace des composants du système à la demande*

| | $PFD_{Low}$ | $PFD_{Medium}$ | $PFD_{High}$ |
|---|---|---|---|
| Détecteur d'hydrogène | 0,0007008 | 0,0032412 | 0,0071832 |
| Unité de traitement logique | 0,0033691 | 0,06822113 | 0,2054623 |
| Vanne d'isolement automatique | 0 | 0,010141331 | 0,047927551 |

Les composant du SIS sont disposés suivant une architecture parallèle-série, la fiabilité du système est donnée par la relation suivante :

$$R_{sys} = \prod_{j=1}^{n}\left[1 - \prod_{i=1}^{n}(1 - R_{ij})\right] \tag{3.4}$$

$$R_{sys} = \left(1 - (1 - R_{détecteur})^{n(1)}\right) \times \left(1 - (1 - R_{LS})^{n(2)}\right) \times \left(1 - (1 - R_{actionneur})^{n(3)}\right) \tag{3.5}$$

Les prix de chaque composant du système sont donnés dans le tableau suivant :

*Tableau 3-4 : Les prix des composants du système*

| Composant | Prix unitaire ($) |
|---|---|
| Détecteur d'hydrogène | 300 |
| Unité de traitement logique | 100 |
| Vanne d'isolement automatique | 100 |

Le coût total du système est donné par la relation :

$$Prix_{sys} = n(1) \times Prix_{détecteur} + n(2) \times Prix_{LS} + n(3) \times Prix_{actionneur} \tag{3.6}$$

## 3.4. Démarche d'optimisation par Algorithmes Évolutionnaires

L'objectif de notre démarche d'optimisation est de trouver une architecture qui permet d'atteindre le SIL requis pour le SIS avec le meilleur prix possible.

Cette problématique se traduit mathématiquement par la minimisation de la fonction coût du système, en agissant sur les variables n(1), n(2) et n(3) qui représentent respectivement le nombre de détecteurs d'hydrogène, le nombre d'unités de traitement logique et le nombre de vannes d'isolement automatique.

La solution retenu doit vérifier les conditions de contraintes imposées par le niveau de fiabilité propre à un SIL de niveau trois.

### 3.4.1. Objectif de l'optimisation

Nous commençons par définir la fonction objective à optimiser ainsi que le type d'optimisation.

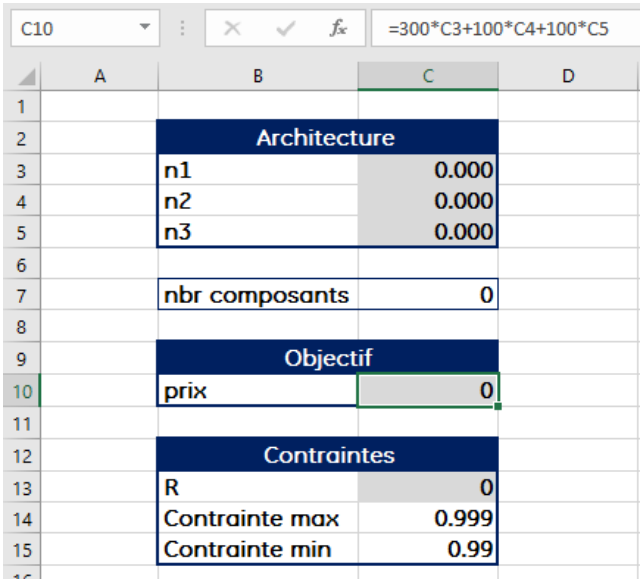


*Figure 3-1 : Définition de la fonction "Objectif"*

Dans notre cas, notre objectif est de minimiser le prix du SIS. Nous essaierons alors de minimiser la fonction 3.6 .

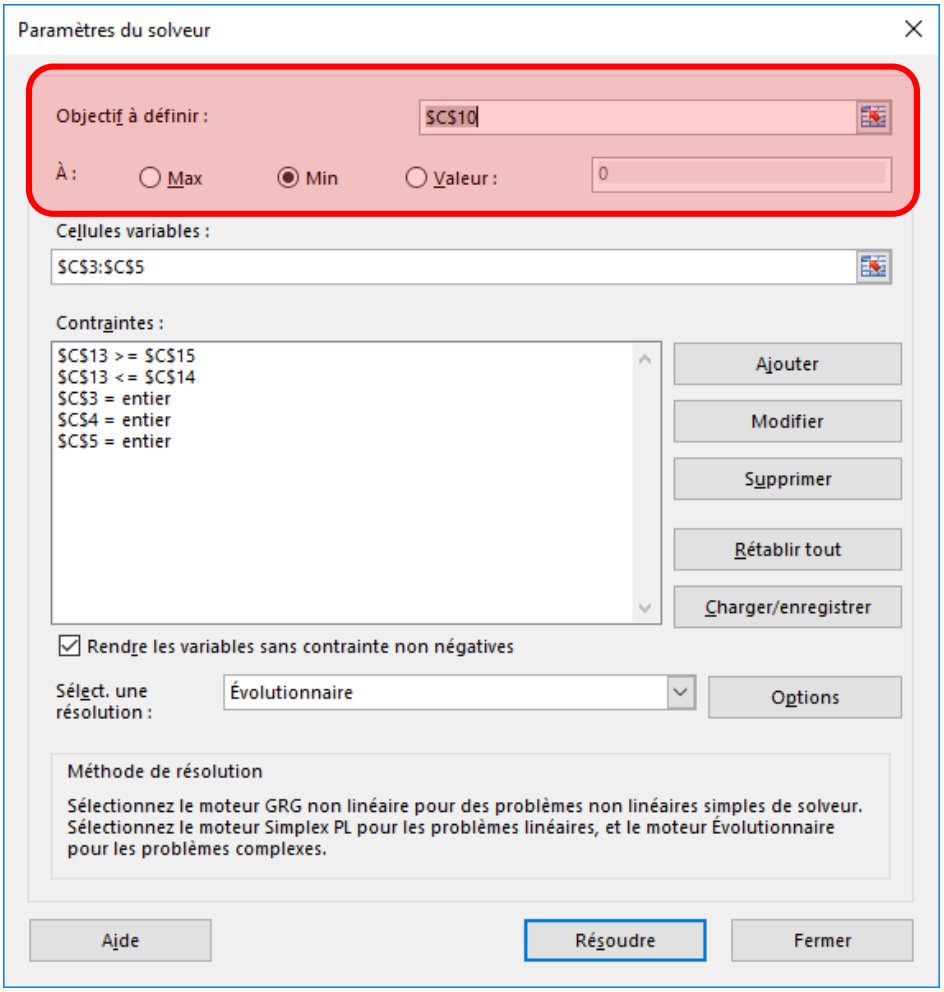


*Figure 3-2 : Minimisation de la fonction "Objectif"*

### 3.4.2. Définition des variables

Dans notre cas, nous allons agir sur le nombre de composant (redondance) dans chaque bloc du SIS

| | | |
|---|---|---|
| n(1) | : | le nombre de détecteurs d'hydrogène |
| n(2) | : | le nombre d'unités de traitement logique |
| n(3) | : | le nombre de vannes d'isolement automatique |

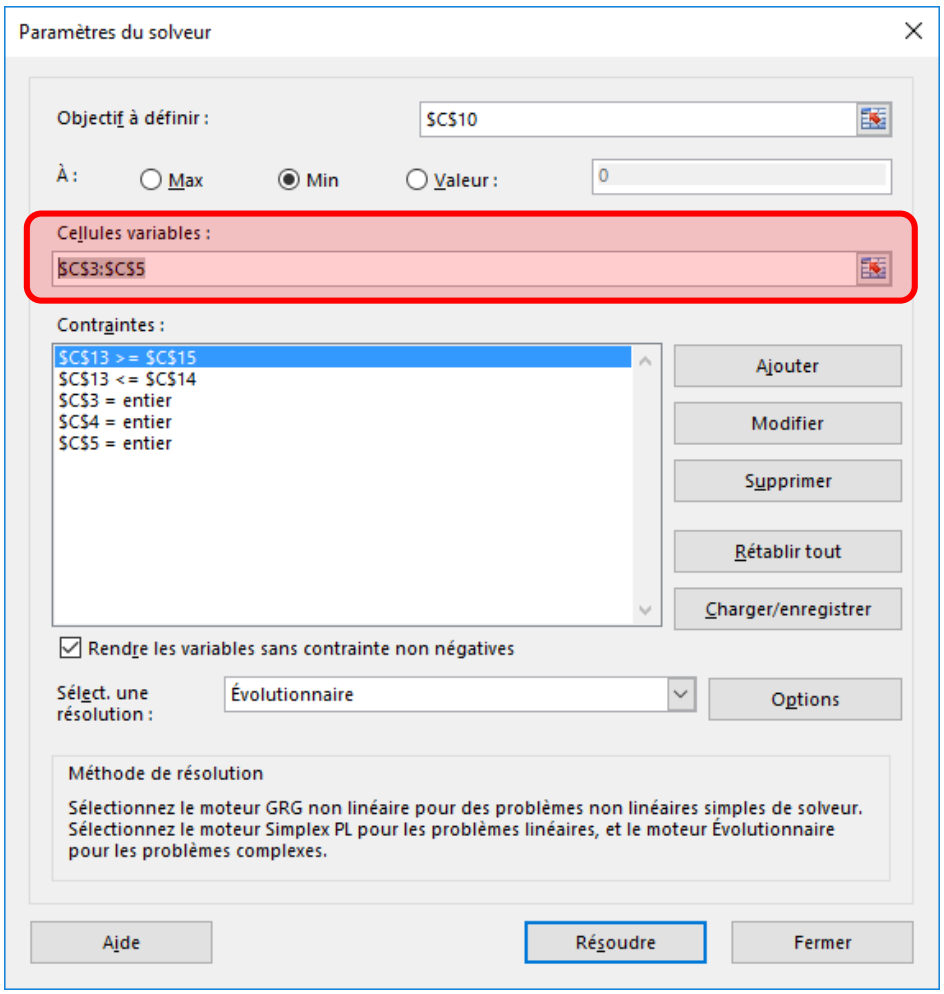


*Figure 3-3 : Définition des variables*

### 3.4.3. Définir les contraintes sur les variables de l'optimisation

Les variables n(1), n(2) et n(3) qui représentent respectivement le nombre de détecteurs d'hydrogène, le nombre d'unités de traitement logique et le nombre de vannes d'isolement automatique. Ils doivent être des nombres entiers.

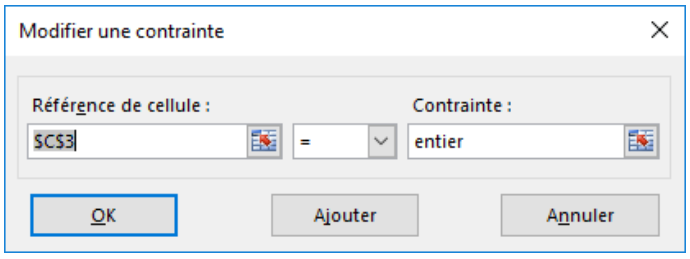


*Figure 3-4 : Variable nombre de détecteurs d'hydrogène.*

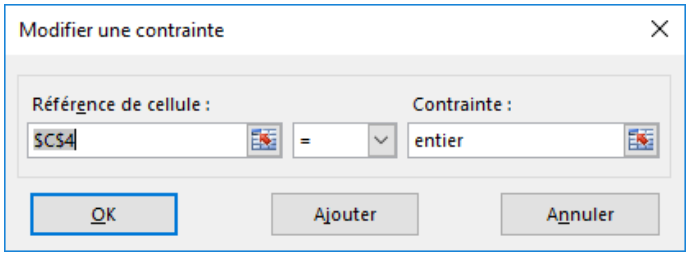


*Figure 3-5 : Variable nombre d'unités de traitement logique.*

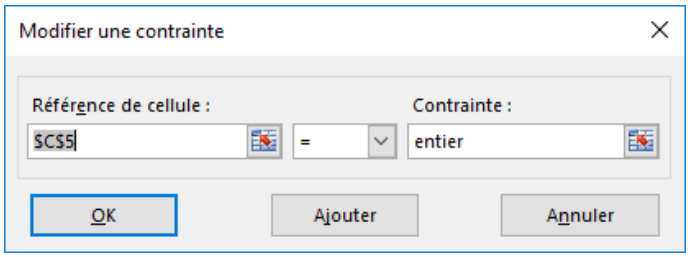


*Figure 3-6 : Variable nombre de vannes d'isolement automatique.*

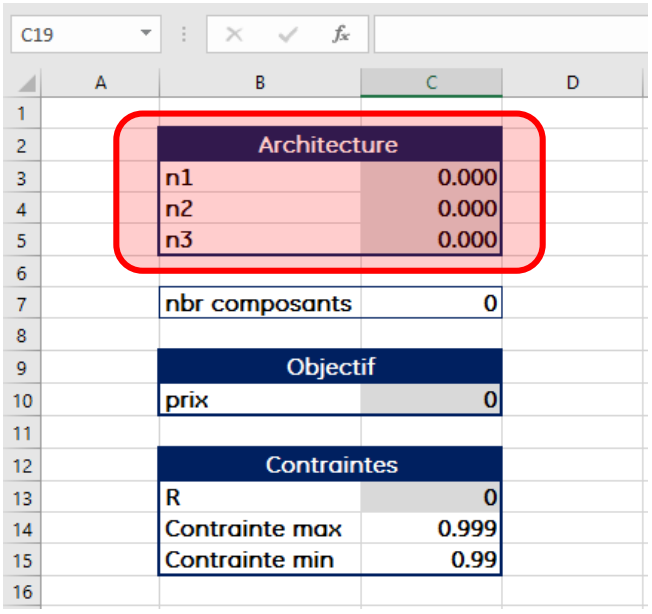


*Figure 3-7 : Variables de l'optimisation.*

### 3.4.4. Définir les contraintes sur l'objectif de l'optimisation

L'architecture optimisés du système doit produire une fiabilité totale du système qui correspond à un niveau d'intégrité de sécurité (SIL) de niveau trois.

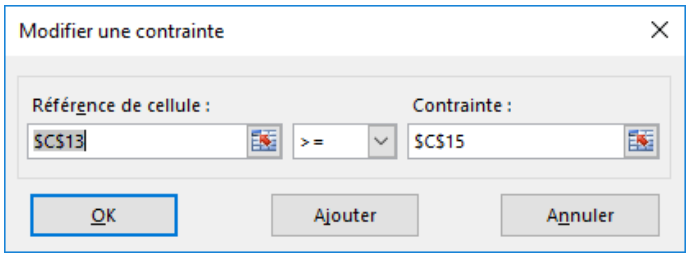


*Figure 3-8 : Contraintes de fiabilité minimale*

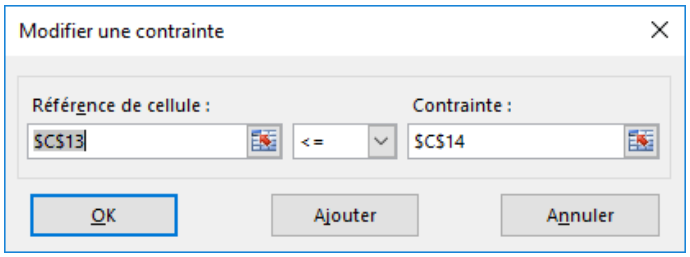


*Figure 3-9 : Contraintes de fiabilité maximale.*

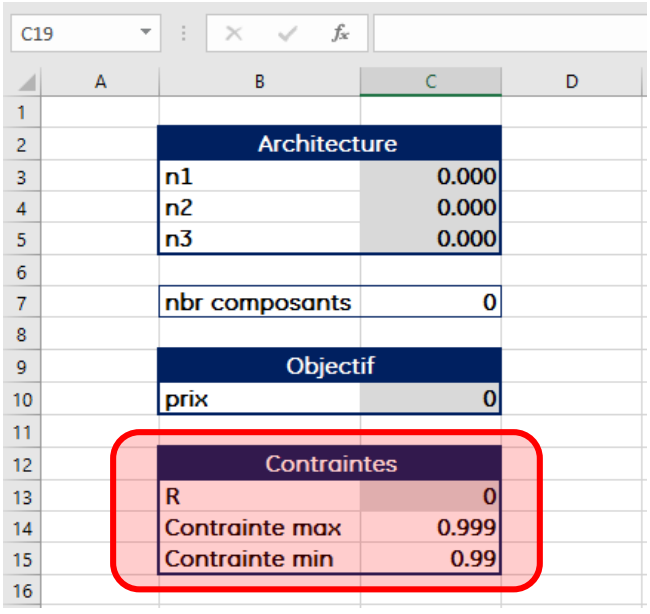


*Figure 3-10 : : Contraintes de l'optimisation*

## 3.5. Résultat d'optimisation par Algorithmes Évolutionnaires

Nous exécutons le calcul d'optimisation au moins du solveur utilisant les algorithmes évolutionnaires.

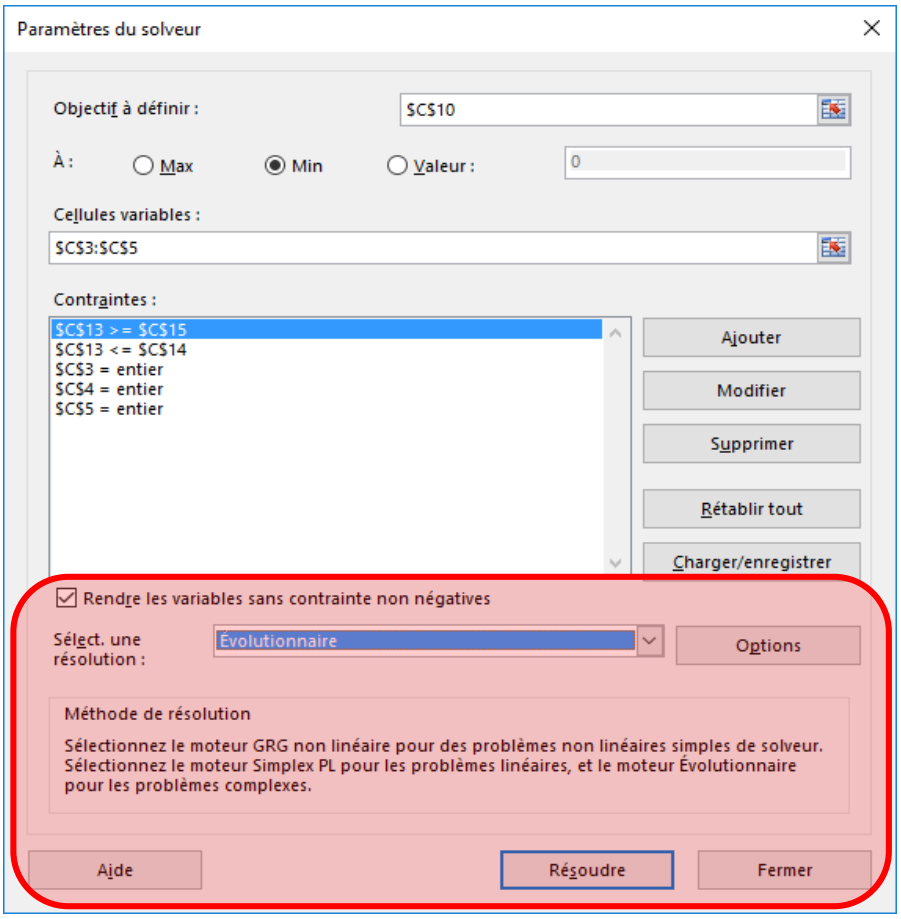


*Figure 3-11 : Exécution du calcul d'optimisation*

L'algorithme propose une première solution intermédiaire qui permet d'avoir une fiabilité de 0.99919 en utilisant 8 composant selon une architecture [ 2 3 3] pour un prix de 1200$.

| Architecture | |
|---|---|
| n1 | 2.000 |
| n2 | 3.000 |
| n3 | 3.000 |

| | |
|---|---|
| nbr composants | 8 |

| Objectif | |
|---|---|
| prix | 1200 |

| Contraintes | |
|---|---|
| R | 0.9991914 |
| Contrainte max | 0.9999 |
| Contrainte min | 0.999 |

*Figure 3-12 : solution intermédiaire*

La solution retenue, après optimisation par les algorithmes évolutionnaires, permet d'avoir une fiabilité de 0.99953 en utilisant 8 composant selon une architecture [ 2 4 2 ] pour un prix de 1200$.

| Architecture | |
|---|---|
| n1 | 2.000 |
| n2 | 4.000 |
| n3 | 2.000 |

| | |
|---|---|
| nbr composants | 8 |

| Objectif | |
|---|---|
| prix | 1200 |

| Contraintes | |
|---|---|
| R | 0.9995389 |
| Contrainte max | 0.9999 |
| Contrainte min | 0.999 |

*Figure 3-13 : solution retenue*

## 3.6. Conclusion

La méthode d'optimisation et de fiabilité des systèmes utilisée nous a permis de satisfaire le niveau de fiabilité structurale requis en déterminant la meilleure conception possible en termes de coût et de qualité.

Les algorithmes évolutionnaires ont manipulé des populations de solutions et ont proposé une première solution intermédiaire qui permet d'avoir une fiabilité de 0.99919 en utilisant 8 composant selon une architecture [ 2 3 3] pour un prix de 1200$.

La solution retenue après optimisation par les algorithmes évolutionnaires propose une architecture utilisant huit composant dans le système instrumenté de sécurité disposés en parallèle-série.

Le système instrumenté de sécurité retenu sera composé de deux détecteurs d'hydrogène, de quatre unités de traitement logique et de deux vannes d'isolement automatique.

Le prix de ce système instrumenté de sécurité est de 1200$. Et la fiabilité » de ce système est évaluée à 0.99953, soit 99.953 % , ce qui répond à un niveau d'intégrité de sécurité (SIL) de niveau trois.

L'architecture du système instrumenté de sécurité étant optimisée, nous proposons de réaliser une étude de la sureté de fonctionnement de ce système par chaines de Markov. Cette étude fera l'objet du chapitre suivant.

# Chapitre 4. Étude du SIS optimisé par chaîne de Markov

# Chapitre 4. Étude du SIS optimisé par chaines de Markov

## 4.1. Introduction

L'approche markovienne est la plus utilisée des méthodes probabilistes mises en œuvre pour le traitement des systèmes se comportant dynamiquement.

Elle entre dans la classe des « *approches analytiques* par *états* » basées sur l'identification des différents états du système concerné puis sur l'analyse de l'évolution du « *système* » entre les *« états »*.

Cette approche ouvre ainsi la voie au traitement de toute une classe d'études orientée vers la sécurité et l'économie.

Dans ce chapitre, nous utiliserons cette approche afin de valider l'architecture du SIS optimisée précédemment.

## 4.2. Description du système à modéliser


*Figure 4-1 : Schema d'un SIS.*

Nous utiliserons les notations suivantes dans la suite de notre étude afin de faciliter la représentation du système :

- A= Bloc des Unités de Traitement Logique (UTL)
- B= Bloc des Unités de Détection
- C= Bloc des Unités d'Actionnement

Lorsque plusieurs composants du SIS sont simultanément en panne, nous considérerons l'ordre de priorité suivant pour la réparation :

| Priorité de réparation A > Priorité de réparation B > Priorité de réparation C |
|---|

De l'état de marche parfait, on peut passer vers un état intermédiaire par défaillance d'un composant du SIS.

D'un état intermédiaire, on peut aller soit vers l'état avale de panne par défaillance d'un autre composant du SIS, ou revenir à l'état amont par réparation du composant défaillant prioritaire.

De l'état de défaillance totale, on peut revenir uniquement vers un état amont par réparation de l'UTL qui est prioritaire pour la réparation.

## 4.3. Identification des états du système considéré

La première étape de construction du graphe de Markov relatif à un système est :

- L'identification des différents états que le système peut occuper au cours de son exploitation.
- La répartition des états rencontrés en deux classes distinctes – Marche/Panne – afin de pouvoir mener à bien les calculs de fiabilité et disponibilité ordinaires.

*Tableau 4-1 : Différents états du SIS.*

| N° état | Description | État du système |
|---|---|---|
| E1 | ABC | Marche parfait |
| E2 | BC | Panne |
| E3 | AC | Panne |
| E4 | AB | Panne |
| E5 | C | Panne |
| E6 | B | Panne |
| E7 | A | Panne |
| E8 | O | Panne totale |

Les symboles (A, B, C) correspondent aux blocs des fonctions du SIS en état de marche.

## 4.4. Identification des transitions :

Une fois la dichotomie réalisée entre les états de marche et de panne, nous devons identifier toutes les transitions possibles entre les différents états de notre système.

Chaque transition symbolise la façon avec laquelle le système passe d'un état vers un autre.

Le but de notre étude est de calculer la fiabilité du système. Afin que le modèle représente la fiabilité du système, il nous faudra faire en sorte qu'aucun chemin aboutissant à l'un des états de marche à l'instant t ne soit jamais passé par un état de panne dans l'intervalle [0, t]. Pour satisfaire cette condition, tous les chemins, permettant de revenir vers un des états de marche à partir d'un état de panne, ne seront pas retenus.

Les transitions possibles entre les états sont :

*Tableau 4-2 : Transitions entre les états*

| État initial (Ei) | Cause de la transition | État final (Ej) |
|---|---|---|
| E1 | Défaillance de A | E2 |
| E1 | Défaillance de B | E3 |
| E1 | Défaillance de C | E4 |
| E2 | Défaillance de B | E5 |
| E2 | Défaillance de C | E6 |
| E3 | Défaillance de A | E5 |
| E3 | Défaillance de C | E7 |
| E4 | Défaillance de A | E6 |
| E4 | Défaillance de B | E7 |
| E5 | Défaillance de C | E8 |
| E6 | Défaillance de B | E8 |
| E7 | Défaillance de A | E8 |

## 4.5. Construction du graphe de Markov

La construction du graphe de Markov passe par :

- La représentation de chacun des états par un cercle,
- La représentation des transitions entre les états par des flèches.

À la fin de cette étape, on se retrouve en présence d'un graphe d'états qui modélise le comportement du système.

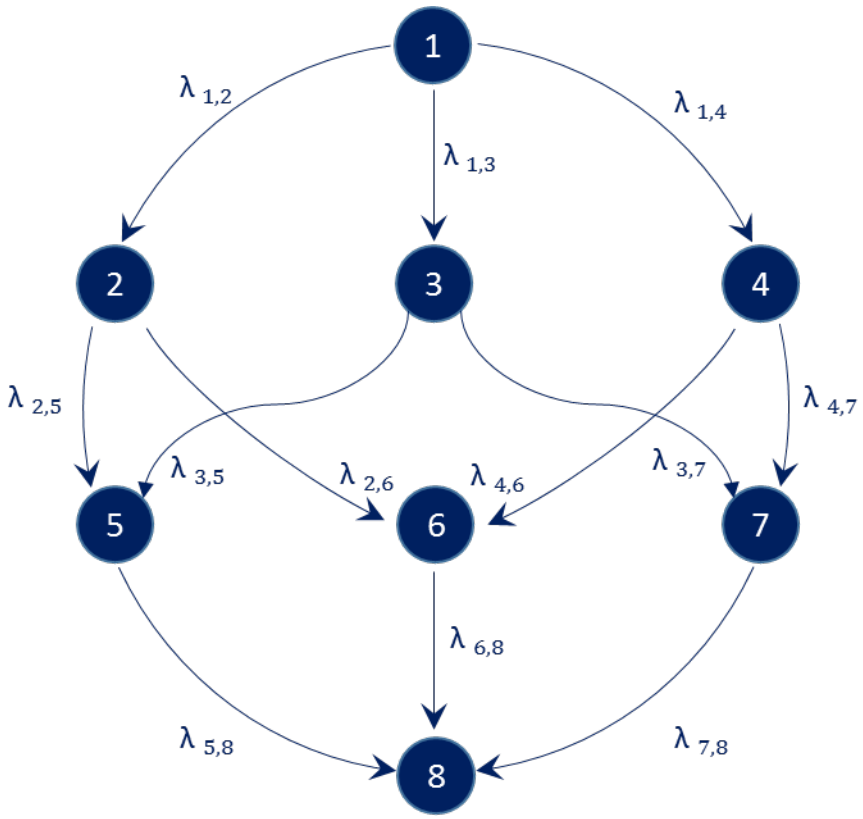


*Figure 4-2 : Graphe de Markov du SIS*

Le graphe obtenu représente, de manière synthétique, tous les chemins (séquences d'événements) que le système peut emprunter à partir de son état initial durant son évolution au cours du temps.

Pour que ce graphe obtenu représente le processus de Markov associé, il reste à préciser quelles sont les chances que chacune de ces transitions soit réellement empruntée au cours de la vie du système. Cela est obtenu en affectant des **taux de transition $\boldsymbol{\lambda_{ij}}$** à chacune d'elles.

Mathématiquement, $\boldsymbol{\lambda_{ij}} \cdot dt$ est la probabilité conditionnelle de sauter de l'état Ei vers l'état Ej entre t et t + dt lorsqu'on est dans l'état Ei à l'instant t.

Les taux de transition correspondent aux **taux de défaillance** des composants qui causent les changements d'état.

Dans le cadre des hypothèses[2] que nous adoptons pour notre étude, les taux de transition sont **constants** et toutes les lois de probabilités qui régissent les divers phénomènes pris en compte sont donc de nature ***exponentielle*** (*processus de Markov homogène).*

[2] Les systèmes et les équipement considérés lors de notre étude de Sûreté de Fonctionnement sont supposés être dans la période de maturité (courbe baignoire).

La probabilité de sauter de Ei vers Ej ne dépend que de la présence dans Ei à l'instant t mais pas de la manière dont on y est arrivé entre 0 et t, le devenir du système ne dépend que de son état à l'instant t. Il s'agit donc d'un processus **sans mémoire**. Cela implique qu'il converge au bout d'un délai plus ou moins long vers un état d'équilibre indépendant des conditions initiales.

Il s'agit ici des caractéristiques fondamentales des processus de Markov homogènes.

## 4.6. Exploitation du graphe de Markov

### 4.6.1. Fiabilité prévisionnelle

Dans la définition de la fiabilité : il faut assurer la continuité du bon fonctionnement du système sur l'intervalle [0, t].

Le graphe précédent ne renferme aucun chemin permettant au système de passer par l'état de panne puis de revenir dans un état de marche. Il décrit donc le comportement d'un système qui ne peut jamais être en état de marche, à un instant donné, en ayant été une ou plusieurs fois en panne auparavant.

Le modèle s'agit donc d'un modèle de fiabilité

La fiabilité R (t) du système étudié est donc égale à la probabilité de se trouver à l'instant t dans l'un des états de marche. La défiabilité D (t) est égale à la probabilité de se trouver dans l'état de panne.

Comme le système ne peut pas se trouver dans plusieurs états à la fois, les huit états (E1, E2, E3 … E8) sont disjoints. Il en résulte :

- P1 (t) + P2 (t) + P3 (t) + P4 (t) + P5 (t) + P6 (t) + P7 (t) + P8 (t) = 1 ;
- R (t) = P2 (t) + P3 (t) + P4 (t) + P5 (t) + P6 (t) + P7 (t) + P8 (t) ;
- D (t) = P1 (t).

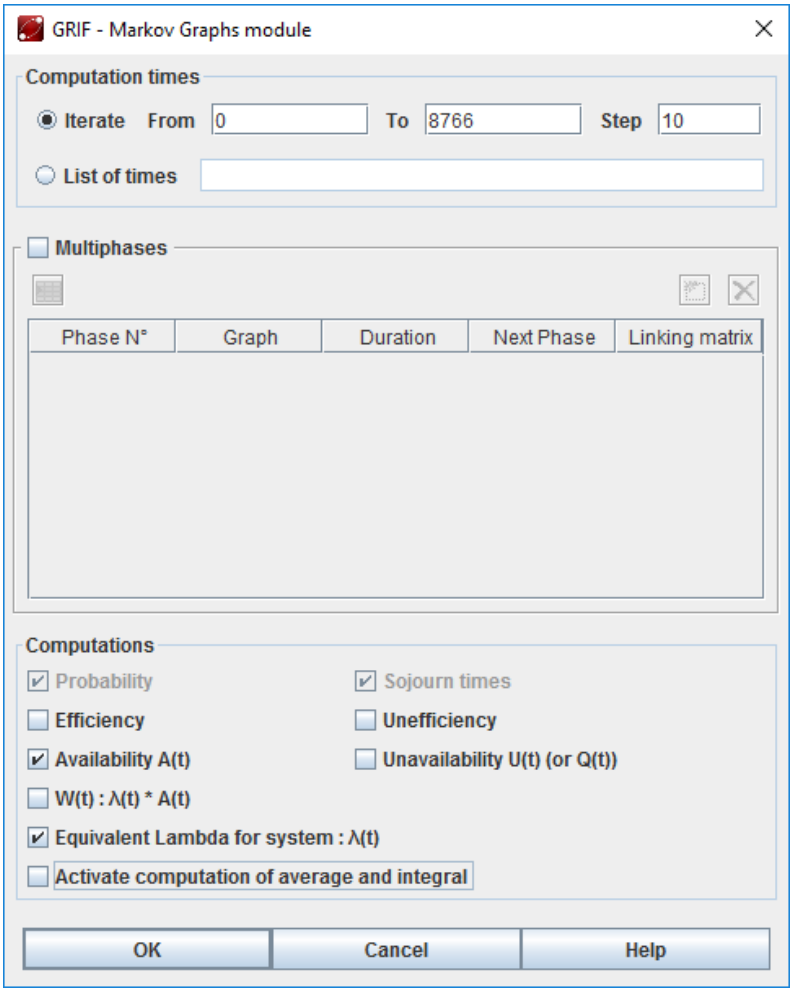


*Figure 4-3 : Calcul de la fiabilité du SIS par graphe de Markov*

Les résultats obtenus sont représentés dans le tableau suivant

*Tableau 4-3 : Résultats du calcul de la fiabilité du SIS*

| État | Fiabilité R(t) |
|---|---|
| ABC | 0.999538877036028 |
| BC | $1.374611 \cdot 10^{-5}$ |
| AC | $7.271007 \cdot 10^{-5}$ |
| AB | $3.746333 \cdot 10^{-4}$ |
| C | $9.999422 \cdot 10^{-10}$ |
| B | $5.152129 \cdot 10^{-9}$ |
| A | $2.725218 \cdot 10^{-8}$ |
| O | $3.747845 \cdot 10^{-13}$ |

Comme il n'existe pas possibilités de sortir de E8, toute la probabilité va se retrouver concentrée dans cet état lorsque le temps va tendre vers l'infini. On dit que l'état E8 est absorbant.

Cela ne fait que traduire la certitude que le système tombe en panne sur une durée infinie. Il en résulte que D (t) tend vers 1 et R (t) vers 0 lorsque le temps t tend vers l'infini.

### 4.6.2. Temps moyens de séjours cumulés.

Au cours de son évolution, le système passe d'état en état et séjourne dans chacun d'eux pendant une certaine durée. C'est le temps moyen de séjour (TMS) observé à chaque passage individuel.

Comme il peut passer plusieurs fois par le même état, nous parlerons de temps moyens de séjour cumulés (TMSC).

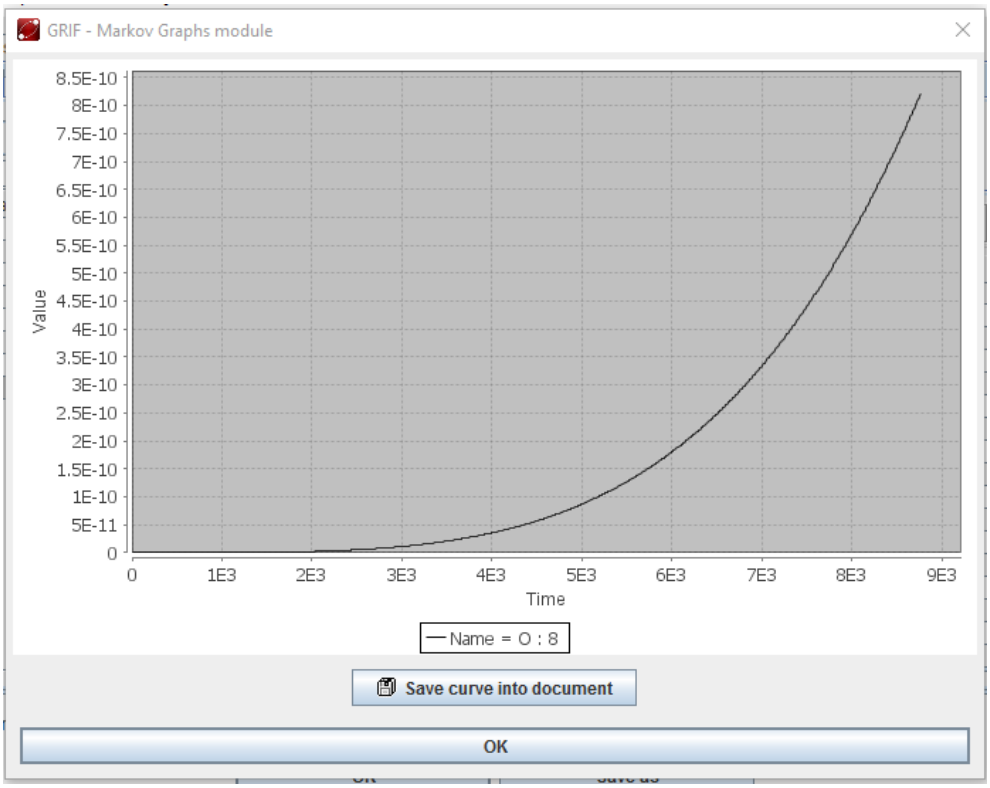


*Figure 4-4 : Le temps moyen de séjour dans l'état O*

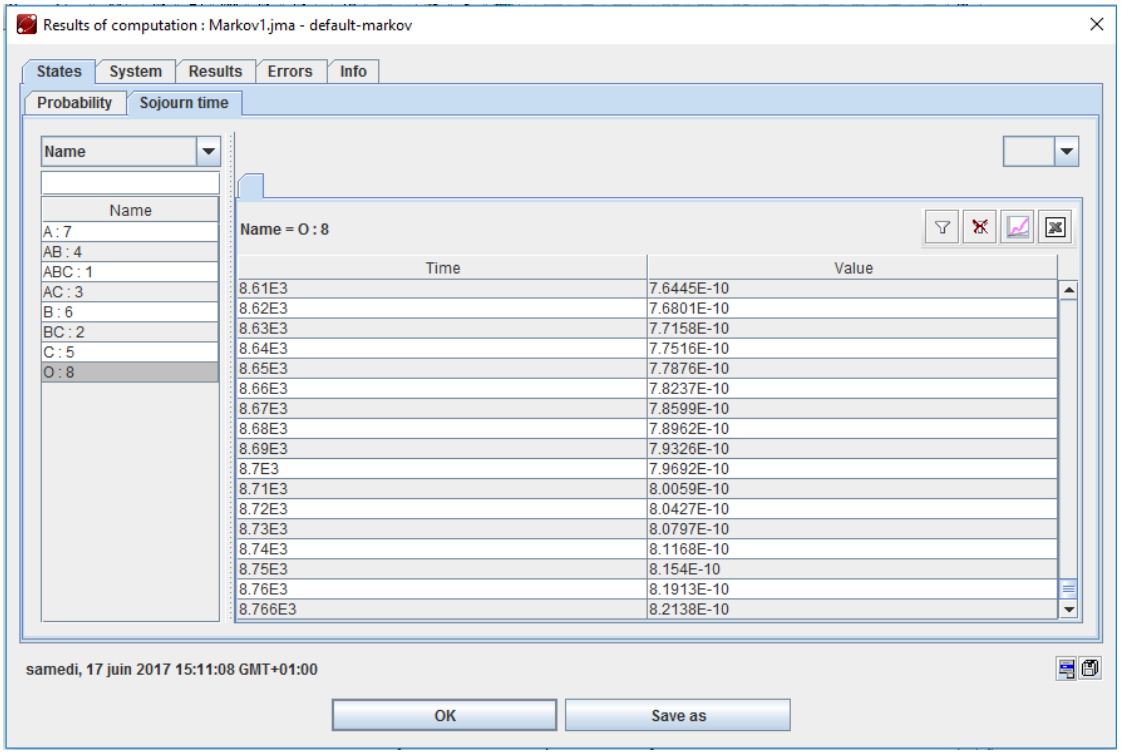


*Figure 4-5 : Résultats de calcul des temps moyens de séjour*

## 4.7. Conclusion

L'étude du Système Instrumenté de Sécurité (SIS) par une approche markovienne nous a permis de compléter notre analyse de la sûreté de fonctionnement du système.

Les résultats obtenus appuient notre choix pour une architecture parallèle-série du Système Instrumenté de Sécurité. En effet, cette étude confirme que l'architecture [ 2 4 2 ] impliquant l'utilisation de deux détecteurs d'hydrogène, quatre Unités de Traitement Logique et deux vannes d'isolement automatique, permet d'atteindre les objectifs de sûreté définis.

Nous avons pu évaluer, par modélisation en chaine de Markov, la fiabilité du système optimisé [ 2 4 2 ] à 0.999538. Cette valeur signifie que le système est fiable à 99,9538%.

La probabilité de défaillance à la demande PFD pour ce système est comprise entre $10^{-4} \leq PFD_{avg} \leq 10^{-3}$. Cette valeur correspond à un Niveau d'intégrité de sécurité (SIL) de niveau trois.

À la fin de ce chapitre, nous avons pu estimer plusieurs paramètre de la sûreté de fonctionnement, comme le taux de défaillance équivalent du système estimé à $\lambda_{sys} = 5{,}261571 \,.\, 10^{-8}$ ainsi que les temps de séjours dans chaque état du système.

# Conclusion

Les systèmes instrumentés de sécurité constituent l'une des barrières de sécurités les plus répandues dans les procédés industriels. Ils représentent une barrière dont l'objectif est de ramener les risques vers des niveaux acceptables. Le niveau de performance de ces SIS doit être proportionnel au niveau de risque dont il a charge de réduire.

La connaissance des notions importantes intervenant dans la sûreté de fonctionnement des équipements nous a permis d'avoir une vision claire sur la démarche à suivre pour répondre aux objectifs fixés par la problématique.

L'optimisation de l'architecture de notre système avait pour objectif la détermination de la meilleure conception possible en termes de coût et de qualité en contrôlant le niveau de fiabilité.

Dans la démarche que nous avons adopté pour la résolution de notre problématique, les algorithmes évolutionnaires, qui s'inspirent de l'évolution des êtres vivants, ont été utilisés comme outil d'intelligence computationnelle exploitant l'intelligence artificielle afin de trouver l'architecture optimale du système.

La méthode d'optimisation et de fiabilité des systèmes utilisée nous a permis de satisfaire le niveau de fiabilité structurale requis en déterminant l'architecture optimale du système.

Les algorithmes évolutionnaires ont manipulé des populations de solutions et ont proposé une première solution intermédiaire qui permet d'avoir une fiabilité de 0.99919 en utilisant 8 composant selon une architecture [2 3 3] pour un prix de 1200$.

La solution retenue après optimisation par les algorithmes évolutionnaires propose une architecture utilisant huit composant dans le système instrumenté de sécurité disposés en parallèle-série. Ce système retenu sera composé de deux détecteurs d'hydrogène, de quatre unités de traitement logique et de deux vannes d'isolement automatique, selon une l'architecture [2 4 2]. Le prix de ce système instrumenté de sécurité est de 1200$.

L'étude du système par une approche markovienne nous permis d'appuyer notre choix pour une architecture parallèle-série. Cette étude confirme que l'architecture [2 4 2] permet d'atteindre les objectifs de sûreté définis. En effet, la fiabilité du système optimisé est évaluée à 0.99953. Cette valeur signifie que le système est fiable à 99,9538%, ce qui correspond à un niveau d'intégrité de sécurité (SIL) de niveau trois.

Finalement, nous avons pu estimer plusieurs paramètre de la sûreté de fonctionnement du système, en évaluant le taux de défaillance équivalent du système estimé à $\lambda_{sys} = 5{,}261571 \,.\, 10^{-8}$ ainsi que les temps de séjours dans chaque état du système.

# Références bibliographiques

Cocozza-Thivent, C. (1997). *Processus stochastiques et fiabilité des systèmes. Berlin: Springer-Verlag Berlin Heidelberg.* Springer, New York.

Davis, L. (1987). *Genetic Algorithms and Simulated Annealing.* Morgan Kaufman, United States.

DE JONG, K. A. (1975). *Analysis of the Behavior of a Class of Genetic Adaptive Systems.* 1975: PhD thesis, University of Michigan, United Stated.

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

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

GOLDBERG, D.E., PELIKAN, M. & LOBO, F.G. (2002). Asurvey of optimization by building and using probabilistic models. *Computational Optimization and Applications, Vol. 21, Issue 1, 5-20.* Springler, Urbana, United States.

GOLDBERG, D. (1989). *Genetic Algorithms in Search, Optimization, and Machine Learning.* Alabama, ADDISON-WESLEY, United States.

HOFFMEISTER, F., & BAECK, T. (1992). *Genetic algorithms and evolution strategies : Similarities and differences.* University of Dortmund, Dortmund.

HOLLAND, J. (1975). *Adaptation in Natural and Artificial System.* Michigan: University of Michigan Press.

IEC 61061. (1998). *Stratifiés de bois densifiés, non imprégnés, à usage électrique.* International Standards Organisation, Geneva.

IEC 61508. (1998). *Functional of electrical/electronic/programmable electronic (E/E/EP) safety related systems.* International Standards Organisation, Geneva.

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

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

KLEINERMAN, M. M., & WEISS, G. H. (1954). On the reliability of networks. *Proceeding of the National Electronics Conference. 10*, pp. 128-136. IEEE, Chicago, Illinois.

LARRANAGA, P., & LOZANO, J. (2002). *Estimation of Distribution Algorithms : A New Tool for Evolutionary Computation.* Kluwer, Boston MA.

LUTTON, E. (2006). Algorithmes génétiques et algorithmes évolutionnaires. *Technique de l'ingénieur*, 5.

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.

MICHALEWICZ, Z. (1992). *Genetic Algorithms + Data Structures = Evolution Programs*, Springer, Berlin Heidelberg.

MUHLENBEIN, H., & PAASS, G. (1996). From recombination of genes to the estimation of distributions. i. binary parameters. In Parallel Problem Solving from Nature. *In: Voigt HM., Ebeling W., Rechenberg I., Schwefel HP. (eds) Parallel Problem Solving from Nature — PPSN IV. PPSN 1996. Lecture Notes in Computer Science, vol 1141* (pp. 178-187). Springer, Berlin.

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

RECHENBERG, I. (1973). *Evolutionsstrategie : Optimierung Technicher System nach Prinzipien der Biologischen Evolution.* Fromman Holzboog, Stuttgart.

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.

SCHWEFEL, H. (1975). *Evolutionsstrategie und numerische Optimierung.* Technische Universität, Berlin.