Conception optimale des Systèmes Instrumentés de Sécurité en présence d'incertitudes

Mohamed Sallak, Jean-François Aubry, Christophe Simon

CONCEPTION OPTIMALE DES SYSTEMES INSTRUMENTES DE SECURITE EN PRESENCE D'INCERTITUDES
OPTIMAL DESIGN OF SAFETY INSTRUMENTED SYSTEMS UNDER UNCERTAINTY

Sallak M. et Aubry J-F.
CRAN-UMR 7039
Nancy université
ENSEM
2 Avenue de la forêt de Haye
54506 Vandoeuvre-Les-Nancy
Tel : 03 83 59 56 47
mohamed.sallak@ensem.inpl-nancy.fr
jean-francois.aubry@isi.u-nancy.fr

Simon C.
CRAN-UMR 7039
Nancy université
ESSTIN
2 Rue Jean Lamour
54519 Vandoeuvre-Les-Nancy
Tel : 03 83 68 51 34
christophe.simon@esstin.uhp-nancy.fr

Résumé
Les Systèmes Instrumentés de Sécurité (SIS) sont des systèmes utilisés pour assurer la sécurité fonctionnelle des installations. Pour concevoir les SIS, deux normes de sécurité sont généralement utilisées : l'IEC 61508 et l'IEC 61511. Cependant, les fiabilistes ont beaucoup de difficultés à mettre en œuvre les prescriptions de ces deux normes pour la conception des SIS qui doivent satisfaire à un niveau d'Intégrité de Sécurité (SIL) exigé. En outre, dans la plupart des travaux d'allocation, on suppose que les données de fiabilité des composants (taux de défaillance, taux de réparation, etc.) fournies par les bases de données sont précis et sans incertitudes. Nous pouvons cependant nous interroger sur leur adaptation à des systèmes hautement fiables pour lesquels les défaillances sont très rares comme les SIS. Dans ce cas, le retour d'expérience est insuffisant pour valider avec précision les taux de défaillance. Parmi les nouveaux défi de la maîtrise de risque et la conception des système de sécurité, la prise en compte de ces incertitudes et la proposition d'autres méthodes que les approches probabilistes classiques (en particulier les ensembles flous) qui peuvent être utilisées avantageusement pour prendre en compte l'imprécision liée à ces taux de défaillance et estimer les probabilités de défaillance des composants ainsi que les disponibilités des SIS lors du processus de conception optimale. L'étude que nous proposons s'inscrit donc dans la conception optimale des SIS en présence d'incertitudes entachant les données de fiabilité des composants.

Summary
A Safety Instrumented System (SIS) is designed for the purpose of mitigating a risk or bringing the process to a safe state in the case of a process failure. However, in the field there is a considerable lack of understanding how to apply the IEC 61508 and IEC 61511 safety standards in order to design SIS to meet the required Safety Integrity Level (SIL). The use of safety related systems imposes to evaluate their dependability. Laboratory data and generic data are often used to provide failure data of safety components to evaluate their dependability parameters. However, due to the lower solicitation of safety systems in plant, safety components have not been operating long enough to provide statistical valid failure data. Furthermore, measuring and collecting failure data have uncertainty associated with them, and borrowing data from laboratory and generic data sources involve uncertainty as well. There are some approaches such fuzzy approaches which may be used to evaluate dependability parameters of safety systems when there is an uncertainty about dependability parameters of systems components. This paper presents an approach for optimal design of SIS under uncertainty.

1. Introduction

Lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont mises en œuvre. Celles-ci participent soit à la prévention en minimisant la probabilité d'apparition du risque, soit à la protection pour limiter les conséquences d'un dysfonctionnement. Les Systèmes Instrumentés de Sécurité (SIS, Safety Instrumented Systems) sont utilisés pour assurer la sécurité fonctionnelle des installations, *i.e.* la réduction des risques à un niveau inférieur ou égal au risque tolérable. Pour concevoir les SIS pour les industries de process, deux normes de sécurité sont utilisées : l'IEC 61508 [1] et l'IEC 61511 [2]. Les fiabilistes ont beaucoup de difficultés à mettre en œuvre les prescriptions de ces deux normes pour la conception des SIS qui doivent satisfaire à un niveau d'Intégrité de Sécurité (SIL, Safety Integrity Level) donné [3][4]. Le SIL exprime la réduction de risque que doit apporter le SIS. Il est certain qu'une stratégie de conception faisant appel à la redondance massive permet en général d'atteindre le SIL exigé, mais avec un coût de mise en œuvre prohibitif. En conséquence, il est primordial de trouver une stratégie d'allocation de paramètres de sûreté de fonctionnement des composants du SIS qui permet d'établir le meilleur compromis entre le SIL requis et le coût de conception du SIS.

Dans la littérature, les méthodes d'allocation de paramètres de sûreté de fonctionnement des composants sont très nombreuses. Elles se différencient par de nombreux points tels que :

- Le paramètre à optimiser : fiabilité, disponibilité, maintenabilité, etc.
- Le type d'architecture considérée : série, parallèle, série parallèle, etc.
- L'approche : soit une approche par pondération ; soit une approche par optimisation. Dans la première, l'objectif de sûreté de fonctionnement est distribué aux composants de l'architecture de telle sorte que l'objectif global soit atteint. Dans la seconde, une solution répondant à des critères d'optimisation en considérant les variables de décision (disponibilités des composants par exemple) est recherchée.
- L'algorithme d'optimisation :
  - Méthodes directes : gradients, programmation dynamique, etc.
  - Heuristiques et méta heuristiques : recuit simulé, recherche tabou, algorithmes génétiques, colonies de fourmis, etc.

Pour prendre en compte les aspects de défaillance des composants, nous nous intéressons à l'allocation de disponibilité. En outre, pour tenir compte du choix limité de composants disponibles sur le marché, nous nous intéressons à l'allocation de redondance. Par conséquent, les travaux de cet article sont orientés vers une stratégie de conception basée sur l'allocation conjointe de disponibilité et de redondance des composants par optimisation. Tillman *et al.* [5] et Tzafestas [6] ont publié des états de l'art sur les techniques d'optimisation de la fiabilité des systèmes. Récemment, Kuo *et al.* [7] ont réactualisé l'ouvrage de Tillman *et al.* [5]. Yalaoui *et al.* [8] ont proposé une méthode d'allocation de fiabilité pour les systèmes séries-parallèles. En ce qui concerne l'allocation conjointe de disponibilité et de redondance, Levitin *et al.* [9] ont proposé une procédure d'optimisation basée sur la minimisation du coût total du système en considérant les taux de défaillance et de réparation des composants, et en agissant sur la fréquence de remplacement et les actions de maintenance corrective et préventive. Castro *et al.* [10] ont également présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de

maintenance. Elegbede *et al*. [11] ont développé une méthodologie d'optimisation de la disponibilité basée sur les plans d'expérience afin de paramétrer l'algorithme génétique utilisé. Nous pouvons ainsi conclure que contrairement à l'allocation de fiabilité, très peu de travaux ont été consacrés à l'allocation conjointe de disponibilité et de redondance. En outre, dans la plupart des travaux d'allocation, on suppose que les données de fiabilité des composants (taux de défaillance, taux de réparation, etc.) peuvent être connues avec précision et validées par le retour d'expérience. Nous pouvons cependant nous interroger sur leur adaptation à des systèmes hautement fiables pour lesquels les défaillances sont très rares comme les SIS. Dans ce cas, le retour d'expérience est insuffisant pour valider avec précision les taux de défaillance. Des méthodes autres que les approches probabilistes classiques (en particulier les ensembles flous) peuvent être utilisées avantageusement pour prendre en compte l'imprécision liée à ces taux de défaillance et être intégrées dans le processus de conception optimale.

L'étude que nous proposons s'inscrit dans le contexte de l'allocation conjointe de la disponibilité et de la redondance des SIS en présence d'incertitudes entachant les données de fiabilité des composants. La méthodologie proposée est basée sur la modélisation fonctionnelle des systèmes par des réseaux de fiabilité. La méthode d'optimisation choisie est celle des algorithmes génétiques. Ce choix est motivé par la présence d'un problème d'optimisation avec une fonction objectif non continue puisque le coût et la disponibilité des SIS sont des valeurs discrètes. En outre, les variables du modèle d'optimisation sont discrètes (nombre et coûts des composants). Or, il n'existe pas de méthodes exactes permettant de résoudre ce type de problème. C'est pourquoi une méthode heuristique ou méta heuristique telle que celle utilisant les algorithmes génétiques est efficace pour résoudre ce problème. D'ailleurs un nombre important de papiers traitant de l'allocation de fiabilité ou de disponibilité par les algorithmes génétiques a été publié [7][10] [11]. A notre connaissance, le problème de conception optimale des SIS en présence d'incertitudes n'a jamais été traité auparavant. En outre, aucun travail d'aide à la conception des SIS n'a été publié jusqu'à présent, d'où la nécessité de proposer une méthodologie de conception des SIS modélisés par des architectures séries parallèles, afin de satisfaire au niveau de SIL exigé en conformité avec les normes de sécurité fonctionnelle IEC 61508 [1] et IEC 61511 [2]. La section 2 présente la procédure proposée par les normes IEC 61508 [1] et IEC 61511 [2] pour l'évaluation de la disponibilité des SIS et l'allocation de SIL. La section 3 présente la procédure de modélisation des probabilités de défaillance floues. La section 4 donne les notions de base de l'étude des réseaux de fiabilité. La section 5 illustre l'algorithme génétique utilisé dans la méthodologie proposée. La section 6 présente l'application retenue ainsi que les paramètres de l'AG et les résultats obtenus à l'aide de notre approche. Enfin, nous concluons sur les perspectives de ce travail.

2. Procédure pour l'évaluation de la disponibilité des SIS et l'allocation de SIL

Dans cette section, nous décrivons la procédure générale pour l'évaluation de la disponibilité des SIS et l'allocation de SIL afin d'assurer la conformité aux normes de sécurité IEC 61511 [2] et IEC 61508 [1].

2.1. Systèmes Instrumentés de Sécurité (SIS)

Un SIS est un système visant à mettre le procédé en position de replis de sécurité (c'est-à-dire un état stable ne présentant pas de risque pour l'environnement et les personnes), lorsque le procédé s'engage dans une voie comportant un risque réel pour le personnel et l'environnement (explosion, feu, etc.).
Un SIS se compose de trois parties :
- Une partie capteur chargée de surveiller la dérive d'un paramètre (pression, température, ...) vers un état dangereux.
- Une partie système de traitement logique chargée de récolter le signal provenant du capteur, de traiter celui-ci et de commander l'actionneur associé.
- Une partie actionneur chargée de mettre le procédé dans sa position de sécurité et de la maintenir.

2.2. Référentiel normatif

La sécurité fonctionnelle a depuis longtemps préoccupé les industriels. Pour mener à bien leur démarche sécurité, ils peuvent s'appuyer sur des normes. La norme internationale de sécurité IEC 61508 [1] est la norme générique dédiée à la sécurité fonctionnelle. Elle est devenue une norme française en 1999. Les normes filles que cette norme de base a généré, sont plus récentes et commencent à être connues des acteurs de la sécurité dans certains secteurs industriels français. Nous nous intéressons en particulier à la norme dérivée IEC 61511 [2] qui est applicable au secteur de l'industrie des procédés. Cet ensemble normatif s'impose comme la référence pour le développement, la mise en oeuvre et l'exploitation des systèmes relatifs aux applications de sécurité.

2.2.1. Norme IEC 61508

La norme IEC 61508 [1] est une norme internationale qui porte plus particulièrement sur les systèmes E/E/P (électriques/électroniques/électroniques programmables de sécurité). La norme propose une approche opérationnelle pour mettre en place un système de sécurité E/E/PE, en partant de l'étude des exigences de sécurité (avec une définition du périmètre couvert, une analyse et une évaluation du risque) et en prenant en compte toutes les étapes du cycle de vie du système E/E/PE.

2.2.2. Norme IEC 61511

La norme IEC 61511 [2] concerne les SIS qui sont basés sur l'utilisation d'une technologie E/E/PE. Elle permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un SIS, de telle manière qu'il puisse être mis en œuvre en toute confiance, et ainsi établir et/ou maintenir les processus dans un état de sécurité convenable. Dans le cas où d'autres technologies sont utilisées pour les unités logiques, il convient aussi d'appliquer les principes fondamentaux de cette norme. Cette norme concerne également les capteurs et les éléments terminaux des SIS, quelle que soit la technologie utilisée.

2.3. Evaluation du niveau d'intégrité de sécurité (SIL)

La norme IEC 61508 [1] fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par le SIS qui exécute les fonctions instrumentées de sécurité exigées. Dans nos travaux, nous supposons que chaque SIS exécute une seule fonction instrumentée de sécurité. La norme IEC 61508 donne le SIL en fonction de la disponibilité moyenne A_{avg} et de sa fréquence de sollicitation pour les SIS faiblement sollicités (moins d'une sollicitation par an) (cf. Tableau 1) et en fonction de probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités ou agissant en mode continu (cf. Tableau 1). Dans cet article, nous nous intéressons uniquement à l'étude des SIS faiblement sollicités. Signalons que la distinction relative à la sollicitation a été retirée de certaines normes. En effet, si certains systèmes sont peu sollicités, leurs défaillances doivent être détectées dans un temps déterminé pour tenir l'objectif de sécurité.

Sollicitation	Demande faible	Demande élevée
SIL	A_{avg}	Défaillances/heure
4	$10^{-5} \leq A_{avg} \leq 10^{-4}$	$10^{-9} \leq N \leq 10^{-8}$
3	$10^{-4} \leq A_{avg} \leq 10^{-3}$	$10^{-8} \leq N \leq 10^{-7}$
2	$10^{-3} \leq A_{avg} \leq 10^{-2}$	$10^{-7} \leq N \leq 10^{-6}$
1	$10^{-2} \leq A_{avg} \leq 10^{-1}$	$10^{-6} \leq N \leq 10^{-5}$

Tableau 1. Définition du niveau de SIL

3. Modélisation des taux de défaillance des composants des SIS

La première question que nous devons nous poser est : comment déterminer les fonctions d'appartenance des taux de défaillance des composants des SIS ? La première étape consiste à modéliser ces taux de défaillance en choisissant les fonctions d'appartenance adéquates.

L'imprécis et l'incertain peuvent être considérés comme deux points de vue sur une même réalité qu'est l'imperfection de l'information concernant les taux de défaillance des composants. Dans ce contexte, nous pouvons différencier clairement les concepts d'imprécis et d'incertain : l'imprécis concerne le contenu de l'information tandis que l'incertain est relatif à sa vérité, entendue au sens de sa conformité à une réalité [12]. Nos travaux proposent seulement un traitement des taux de défaillance imprécis en utilisant des nombres flous sous la forme d'ensembles de valeurs avec des informations de caractère vague. Dans la langue française, il y a d'autres qualificatifs qui renvoient à l'imprécis, tels que "vague", "flou", "général" et "ambigu". L'ambigu est une forme d'imprécision liée au langage. Une information est ambiguë dans la mesure où elle renvoie à plusieurs contextes ou référentiels possibles. Ce type d'imprécision n'est pas celui qui sera considéré dans ce mémoire : nous supposons connu le référentiel associé à l'élément d'information. Le "général" est une forme d'imprécision liée au processus d'abstraction ; une information est générale si elle désigne un ensemble d'objets dont elle souligne une propriété commune. Nous nous intéressons au caractère vague ou flou d'une information qui réside dans l'absence de contours bien délimités de l'ensemble des valeurs affectées aux objets qu'elle concerne. Considérons par exemple, un composant dont le taux de défaillance est obtenu à partir d'une base de données de fiabilité [13][14]. Ce taux de défaillance est donné sous forme d'une valeur moyenne m est d'un facteur d'erreur e. Nous pouvons dire que le taux de défaillance du composant est d'environ m défaillances par an. Dans ce cas, l'information sur le taux de défaillance du composant est vague ou floue. L'imperfection de cette information est considérée comme une imprécision qui sera, par exemple, modélisée par un nombre flou de valeur modale m et de support 2e. Nous proposons donc de modéliser les taux de défaillance imprécis par des nombres flous triangulaires (cf. figure 1) d'extrémité à gauche a (valeur inférieure), d'extrémité à droite b (valeur supérieure) et de valeur modale m. Le paramètre $\mu_{\tilde{A}}(x)$ utilisé dans les figures désigne le degré d'appartenance de chaque valeur x à A.

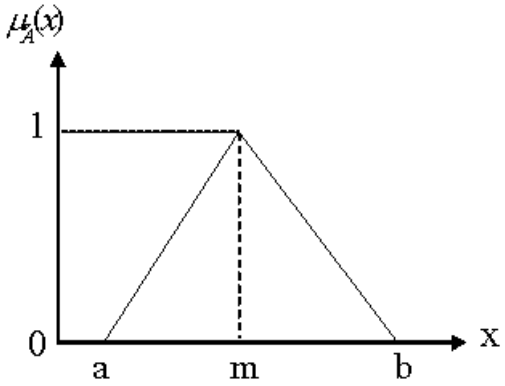

Figure 1. Taux de défaillance flou

Puisque les SIS sont des systèmes à défaillances rares, en utilisant l'approximation des événements rares [Collet, 1996], nous obtenons donc la probabilité floue triangulaire de défaillance d'un composant à partir de son taux de défaillance à un instant t :

$$P(t) = 1 - \exp(-\lambda.t) \approx \lambda.t$$

4. Réseaux de fiabilité

Dans cette section, nous allons présenter les réseaux de fiabilité tels qu'ils ont été définis par Kaufmann *et al.* [15].

4.1. Rappel sur la théorie des graphes

De manière générale, un graphe permet de représenter la structure et les connexions d'un ensemble complexe en exprimant les relations entre ses éléments.
Considérons un ensemble fini *S* et le produit *SxS*. Soit *U* un sous ensemble de *SxS*. Le couple :

$$G = (S, U)$$

est appelé un multi graphe (ou encore graphe *r*-appliqué) où *r* est le nombre maximal des arcs ayant même extrémité initiale et même extrémité terminale. Les éléments de *S* sont appelés les sommets du graphe. Les éléments de *U*, qui sont des couples de sommets, sont appelés les arcs du graphe.

4.2. Concepts de base des réseaux de fiabilité

Un réseau de fiabilité *R* défini sur un ensemble $e = \{e_1, e_2, \ldots, e_i\}$ de composants est constitué par :

- Un graphe *r*-appliqué *G* = (*S, U*) sans boucles, dans lequel deux sommets *O* et *Z* de *S* sont distingués et appelés respectivement "origine" et "extrémité".
– Une application Δ : *U* -> *e* telle que :
$\Omega(u_j) = (S_i, S_k)$, $\Omega(u_{j'}) = (S_i, S_k) \Rightarrow \Delta(u_j) \neq \Delta(u_{j'})$
Où Ω est l'application qui fait correspondre à chaque arc le couple de ses extrémités.

A tout sous-ensemble de composants e_i *de e*, nous pouvons faire correspondre le graphe partiel $G_p(e_i)$ du graphe *G*, obtenu en ne conservant que les arcs de G auxquels correspond un composant appartenant à e_i :

$G_p(e_i) = (S, U_p(e_i))$ (5)

avec : $U_p(e_i) = \{u \in U / \Delta(u) \in e_i\}$. Nous appellerons "lien" d'un réseau *R* un sous-ensemble de composants *a de e* tel qu'il existe dans le graphe *Gp*(*a*) un chemin de *O* à *Z*. Un lien *a* est minimal si aucun sous-ensemble *a' de a* n'est un lien du réseau.

Nous appellerons "coupe" d'un réseau *R* un sous ensemble de composants *b* de *e* tel que le sous-ensemble d'arcs *Up*(*b*) contienne une coupe du graphe *G* relative à un sous-ensemble de sommets incluant *Z* et n'incluant pas *O*. Une coupe *b* est minimale si aucun sous ensemble *b' de b* n'est une coupe du réseau. Un réseau de fiabilité n'est pas un schéma de connexion physique des éléments mais seulement un modèle formelle du comportement dysfonctionnel; si nous connaissons toutes les coupes ou tous les liens alors nous avons deux réseaux de fiabilité équivalents.

4.3. Pourquoi les réseaux de fiabilité ?

La raison principale est que les réseaux de fiabilité permettent de modéliser tout type de structure complexe. Par exemple, la structure représentée dans la figure 2-a ne peut pas être représentée par la structure série parallèle de la figure 2-b (il manque une connexion entre *A* et *D*. Elle peut cependant être représentée par le réseau de fiabilité de la figure 3. La deuxième raison est que suite à l'utilisation des réseaux de fiabilité, nous pouvons utiliser les matrices booléennes de connexion dans le processus d'optimisation. En effet, il est plus aisé de procéder à une optimisation sur une matrice qui est une représentation de la structure du système.

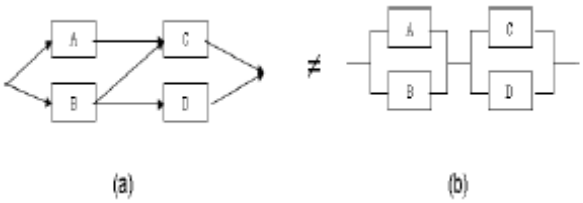

Figure 2. Schéma de connexion et structure série-parallèle

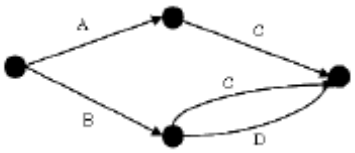

Figure 3. Réseau de fiabilité correspondant à la figure 2-a

4.4. Calcul de la disponibilité moyenne d'un SIS

La disponibilité moyenne A_{avg} du SIS représenté par un réseau de fiabilité est calculée à partir des liens *li* minimaux du réseau de fiabilité. La disponibilité instantanée est définie par l'équation :

$$A(t) = \sum_{i=1}^{n} P_{li(t)}$$

Où :
$P_{li}(t)$ est la disponibilité instantanée du lien minimal *i*.
n est le nombre de liens minimaux du réseau de fiabilité.
En procédant à une disjonction des différents termes qui figurent dans les liens minimaux, nous obtenons :

$$A(t) = P_{l1}(t) + \overline{P}_{l1}(t)P_{l2}(t) + ... + \overline{P}_{l1}(t)\overline{P}_{l2}(t)...\overline{P}_{\ln-1}(t)P_{\ln}(t)$$

Le calcul de disponibilité moyenne A_{avg} du SIS est donné par :

$$A_{avg} = \frac{1}{T}\int_{0}^{T} A(t)dt$$

Où *T* est la période d'étude.

4.5. Calcul de la disponibilité moyenne d'un SIS en présence d'incertitudes

A l'aide de l'opérateur arithmétique flou d'addition, le nombre flou qui représente la disponibilité moyenne A_{avg} du SIS est calculé à partir des nombres flous qui représentent les disponibilités des liens minimaux li du réseau de fiabilité. Les disponibilités des liens minimaux li sont calculées à partir des probabilités floues de défaillance des composants :

$$\mu_{\tilde{A}(t)}(x) = \sum_{i=1}^{n} \mu_{\tilde{P}(li)(t)}(x)$$

Où $\tilde{P}(li)(t)$ est la disponibilité instantanée floue du lien minimal li.

Nous procédons après à la défuzzification de pour obtenir une valeur précise de la disponibilité instantanée :

$$A(t) = defuzz(\mu_{\tilde{A}(t)}(x))$$

Enfin, la disponibilité moyenne A_{avg} du SIS est obtenue en intégrant la disponibilité instantanée sur la période d'étude T :

$$A_{avg} = \frac{1}{T}\int_{0}^{T} A(t)dt$$

5. Algorithme génétique

5.1. Introduction

Pour résoudre les problèmes d'optimisation, 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 (algorithmes génétiques (AG), recuit simulé,…), 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 et dépendent beaucoup du point de départ de recherche de l'extremum. Développés par Holland [16] à l'université du Michigan, les algorithmes génétiques (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 function) [16]. Dans cet article, on propose l'utilisation des AG pour les raisons suivantes :

- La première raison est que la mise en oeuvre 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 continue.
- La deuxième raison est que les AG permettent un équilibre entre exploitation et exploration [16]. 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 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 [7].

5.2. 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, Chen *et al.* [17] ont 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 qu'on a choisie.

5.3. Eléments de l'AG

Nous détaillons par la suite les éléments de l'AG que nous avons utilisés.

5.3.1 Codage des solutions

Dans un AG, on ne travaille pas directement avec les solutions possibles 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. Le codage que nous avons utilisé est un codage en valeurs réelles. Dans ce type de codage, les gènes sont directement les valeurs recherchées. Les chromosomes ici sont définis comme étant des chaînes codant le nombre de composants dans chaque sous systèmes.

5.3.2 Population initiale

Une fois le codage choisi, une population initiale formé de solutions admissibles (chromosomes) du problème doit être déterminée. Plusieurs mécanismes de génération de la population initiale sont utilisés dans la littérature. Nous avons choisi ici la génération aléatoire de la population initiale.

5.3.3 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. Nous avons choisi ici une population de 200 individus.

5.3.4 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. Il existe plusieurs types de sélection [16]. Nous retenons ici la méthode du tournoi binaire stochastique, qui est sans doute aujourd'hui la technique de sélection la plus populaire en raison de sa simplicité et de son efficacité. A chaque fois qu'il faut sélectionner un individu, cette méthode consiste à tirer aléatoirement deux individus de la population, sans tenir compte de la valeur de leur fonction d'adaptation, et de choisir le meilleur individu parmi les deux individus. L'opération est évidemment répétée autant de fois que l'on a de parents géniteurs à sélectionner.

5.3.5 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 génèrent deux enfants. Nous avons choisi ici un croisement à deux points et une probabilité de croisement $P_C=0.5$. Nous coupons le chromosome en deux points choisis aléatoirement et recombinons les morceaux en croisant les chromosomes. Une probabilité de croisement P_C signifie que, quand deux parents sont candidats à la reproduction, on tire un réel *x* aléatoirement selon une loi uniforme sur l'intervalle *[0, 1]*, si *x* est inférieur à P_C, on croise alors les parents.

5.3.6 Mutation

L'opérateur de mutation permet d'introduire un facteur aléatoire dans les solutions générées, et d'élargir ainsi l'espace des solutions explorées 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. La mutation choisie ici consiste à tirer aléatoirement un seul gène dans le chromosome et à le remplacer par une valeur aléatoire avec une probabilité de mutation $P_m=0.03$.

6. Application

En guise d'illustration, nous appliquons la méthodologie proposée à la conception d'un SIS défini dans le document ISA-TR84.00.02-2002 [18] relatif à la norme IEC 61508. Ce SIS doit satisfaire à un SIL *3* exigé avec un coût de conception minimal et un choix réduit de composants.

6.1 Présentation du système

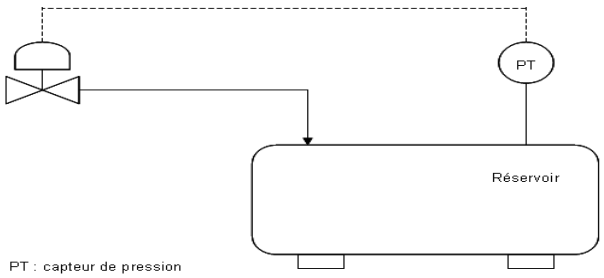

Figure 4. Réservoir sous pression

Nous considérons un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil (cf. Figure 4) [18]. Ce réservoir peut rejeter des gaz dans l'atmosphère. Nous supposons que le risque acceptable est défini sous forme d'un taux moyen de rejet de gaz inférieur à 10^{-4} par an. Une analyse des phénomènes dangereux liés à ce système a montré que les systèmes de protection disponibles (alarmes et niveaux de protection) sont insuffisants pour assurer ce risque acceptable (le non dépassement du seuil imposé pour le rejet des gaz) et qu'une fonction instrumentée de sécurité doit être implémentée dans un SIS pour réduire le taux de rejet du réservoir. Notre objectif est de concevoir ce SIS pour qu'il réalise la fonction instrumentée de sécurité, avec un coût total minimal et qui ne dépasse pas le coût maximal C_{max}.

6.2. Formulation du problème

6.2.1 Notations

Pour formuler le problème d'allocation conjointe de redondance et de disponibilité du SIS, nous allons utiliser les notations données dans le tableau 2. Le SIS est constitué de trois sous systèmes :

- Sous système Capteurs,
- Sous système Unités de traitements,
- Sous système Actionneurs.

6.2.2. Interprétation des objectifs

Nous désirons avoir un niveau de SIL *3* avec un coût total minimal. Selon le Tableau 1, nous obtenons par exemple pour le SIL1 la contrainte suivante : $SIL1 \rightarrow 0.999 \leq A_{avg} \leq 0.9999$

Chaque sous système peut contenir un ou plusieurs composants du même type en redondance. Pour chaque sous-système du SIS, nous avons un nombre donné de composants disponibles.
Nous cherchons donc le nombre de composants utilisés dans chaque sous-système *i* afin d'obtenir la fonction instrumentée de sécurité de SIL *3* avec un coût total C_S minimal et ne dépassant pas C_{max}=25000. C'est à dire qu'il faut trouver les n_C, n_U, n_a afin de :
Minimiser CS
Sous les contraintes :

$$A_{avg\min} \le A_{avg} \le A_{avg\max}$$

$$C_S \le C_{\max}$$

$$n_{C\min} \le n_C \le n_{C\max}$$

$$n_{U\min} \le n_U \le n_{U\max}$$

$$n_{a\min} \le n_a \le n_{a\max}$$

Symbole	Signification
S_i	Sous-système i
k_i	Capteur i
l_i	Unité de traitement i
m_i	Actionneur i
n_C	Nombre de capteurs disponibles
n_U	Nombre d'unités de traitement disponibles
n_a	Nombre d'actionneurs disponibles
A_{avg}	Disponibilité moyenne du SIS
C_s	Coût total du SIS

Tableau 2. Notations utilisées pour la formulation des critères d'optimisation

Le tableau 3 présente les valeurs des taux de défaillance flous (les paramètres a, m et b) ainsi que le nombre de composants disponibles pour chaque sous-système du SIS et les coûts. Les valeurs des données de fiabilité ainsi que le coût des composants sont conformes à ceux utilisées sur le marché [3]. Les paramètres retenus de l'algorithme génétique sont donnés dans le tableau 4. Les figures 5 et 6 donnent les configurations obtenues pour l'obtention du SIL 3.

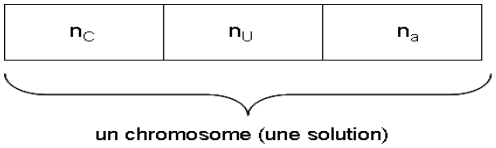

Figure 5. Codage d'une solution

&²

Capteurs	a_i	m_i	b_i	Coût
Type 1	0.017	0.039	0.059	2100
Type 2	0.065	0.07	0.08	1500
Type 3	0.02	0.03	0.05	2000

Unités de traitement	a_i	m_i	b_i	Coût
Type 1	0.086	0.09	0.092	1400
Type 2	0.048	0.05	0.052	2100
Type 3	0.065	0.07	0.076	1200

Actionneurs	a_i	m_i	b_i	Coût
Type 1	0.086	0.1	0.11	2500
Type 2	0.057	0.06	0.061	3500
Type 3	0.038	0.04	0.042	4100

Tableau 3. Taux de défaillances et coûts des composants

Paramètres	Valeurs
Type de codage	Codage réel
Taille de la population	200
Méthode de croisement	Croisement à deux points
Probabilité de croisement	0.5
Méthode de mutation	Mutation aléatoire d'un seul gène
Probabilité de mutation	0.03
Méthode de sélection	Tournoi binaire stochastique
Nombre de générations	150

Tableau 4. Paramétrage de l'algorithme génétique

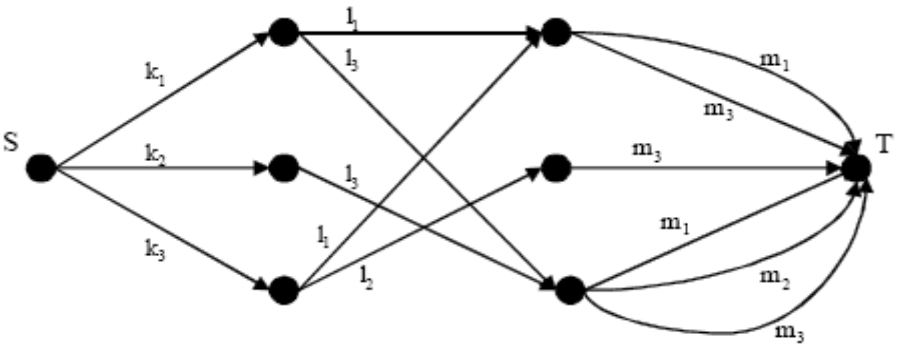

Figure 5. Architecture obtenue (SIL3 : A_{avg} = 0.99906, C = 20400) : Réseau de fiabilité

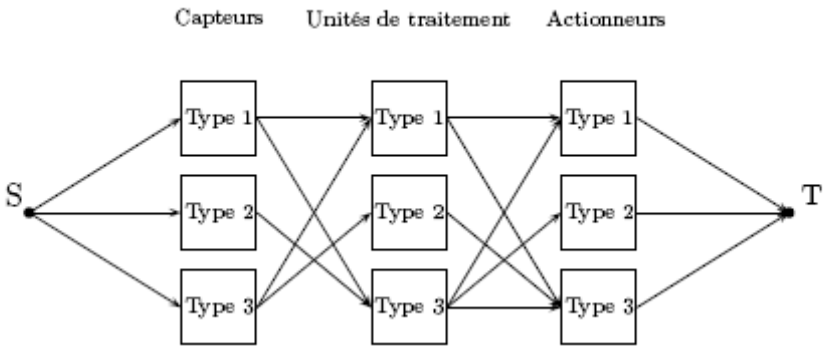

Figure 6. Architecture obtenue (SIL3 : A_{avg} = 0.99906, C = 20400) : Schéma de connexion

Pour le SIL 3 exigé, l'AG converge vers la solution optimale à partir de 115 générations. En outre, la configuration obtenue respecte la contrainte du coût (C_{max} = 25000 euros). En pratique, il faudrait ajouter un voteur à chaque sous système du SIS pour que l'architecture du SIS soit plus conforme aux SIS proposés actuellement dans le marché. Les voteurs reçoivent les valeurs envoyées par chaque composant en redondance du sous système où ils sont installés. Ensuite, ils envoient la valeur, pour laquelle tous les composants en redondance sont d'accord, aux composants du sous système adjacent. Dans les solutions que nous avons proposées, nous avons supposé que les voteurs font partis des composants (capteurs, unités de traitement et actionneurs).

7. Conclusion

Nous avons proposé une méthodologie de conception optimale des SIS qui doivent satisfaire au niveau d'intégrité de sécurité (SIL) exigé par les normes de sécurité IEC 61508 et IEC 61511 en présence d'incertitudes sur les données de fiabilité des composants. Les résultats obtenus sont satisfaisants et les configurations obtenues respectent les contraintes imposées.

Des paramètres additionnels peuvent être pris en considération au niveau du modèle (causes communes de défaillances, taux de couverture du diagnostic, etc.). Nous pouvons aussi obtenir une stratégie optimale en raisonnant non seulement sur les taux de défaillance mais aussi sur les taux de réparation des composants et les politiques de maintenance préventives et correctives des SIS.

Références

[1] IEC 61508, Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems, International Electrotechnical Commission (IEC), 1998.
[2] IEC 61511, Functional safety: Safety Instrumented Systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.
[3] Goble W. M. and H. Cheddie. Safety Instrumented Sytems Verification- Practical Probabilistic Calculations. ISA, 2006.
[4] Sallak M., 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, 2007.
[5] Tillman F.A., C.L. Hwang, and W. Kuo, 1980. Optimization of systems reliability, Marcel Dekker, NY.
[6] Tzafestas S.G., Optimization of system reliability: A survey of problems and techniques, International Journal System Science, 11, p. 455-486, 1980.
[7] Kuo W., Prasad V.R, Tillman F.A., Hwang C.L., Optimal Reliability Design: Fundamentals and applications, Cambridge, University Press, 2001.
[8] A. Yalaoui, E. Chatelet, and C. Chengbin, "A new dynamic programming method for reliability and redundancy allocation in a parallel-series system," IEEE Transactions on Reliability, vol. 54, pp. 254–261, 2005.
[9] Levitin G. and A. Lisnianski, Joint redundancy and maintenance optimization for multi-state series-parallel systems, Reliability Engineering and System Safety, 64, p. 33-42, 1999.
[10] Castro H.P. and K.L. Cavalca. Availability optimization with genetic algorithm, International Journal of Quality and Reliability Management, 20, p. 847-863, 2003.
[11] Yang J-E., M-J. Hwang, T-Y. Sung and Y. Jin, Application of genetic algorithm for reliability allocation in nuclear power plants, Reliability Engineering and System Safety, p. 229-238, 1999.
[12] B. Bouchon-Meunier. La logique floue et ses applications. Vie artificielle. 1995.
[13] CCPS. Offshore reliability data handbook, 4th Edition. 2002.
[14] IEEE. IEEE guide to the collection and presentation of electrical, electronic, sensing component, and mechanical equipement reliability data for nuclear-power generating station. IEEE-std-500, 1984.
[15] A. Kaufmann, D. Grouchko, and C. Cruon. Mathematical models for the study of the reliability of systems. New York: Academic Press, 1977.
[16] Holland J. H., Adaptation in natural and artificial systems, University of Michigan press, 1975.
[17] Chen J., E. Antipov, B. Lemieux, W. Cedeno and D. H. Wood, DNA computing implementing genetic algorithms. In L. F. Landweber, E. Winfree, R. Lipton, and S. Freeland, editors, Evolution as Computation, p. 39-49, New York. Springer Verlag, 1999.
[18] ISA-TR84.00.02-2002. Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation Techniques. Instrumentation Society of America (ISA), 2002.