Allocation conjointe de redondance et de disponibilité des Systèmes Instrumentés de Sécurité

Une approche par les blocs diagrammes de fiabilité

Mohamed Sallak* — Christophe Simon — Jean-François Aubry***

** Centre de Recherche en Automatique de Nancy, Nancy Université, CNRS, 2 Avenue de la forêt de Haye, 54506 Vandœuvre lès Nancy*

mohamed.sallak@ensem.inpl-nancy.fr ; jean-francois.aubry@isi.u-nancy.fr

*** Centre de Recherche en Automatique de Nancy, Nancy Université, CNRS, 2 Rue Jean Lamour, 54519 Vandœuvre lès Nancy*

christophe.simon@esstin.uhp-nancy.fr

RÉSUMÉ. Cet article propose une méthodologie de conception optimale des Systèmes Instrumentés de Sécurité (SIS) afin de satisfaire au niveau d'Intégrité de Sécurité (SIL) exigé par les normes de sécurité IEC 61508 et IEC 61511. L'étude proposée s'inscrit dans le contexte de l'allocation conjointe de disponibilité et de redondance des composants des SIS. Elle est basée sur la modélisation des SIS par des systèmes séries parallèles sous forme de blocs diagrammes de fiabilité. Un algorithme génétique (AG) est utilisé pour optimiser le coût de conception du SIS sous contrainte de disponibilité en fonction des objectifs de SIL. L'objectif consiste à rechercher la meilleure architecture série parallèle à partir d'un jeu de composants type. La méthodologie est appliquée à la conception d'un SIS défini dans le document ISA-TR84.00.02-2002 relatif à la norme IEC 61508. Nous expérimentons cette approche avec des objectifs de SIL allant de 1 à 4.

ABSTRACT. This paper presents an optimal design of Safety Instrumented Systems (SIS) to achieve the required Safety Integrity Level (SIL) according to IEC 61508 and IEC 61511 safety standards. The methology is based on a redanduncy and avalaibility allocation of SIS components. The optimal allocation proposed the use of reliability blocs diagrams and genetic algorithms (GA). An example from the ISA-TR84.00.02-2002 which illustrates the use of the allocation model to achieve a SIL i (i=1, 2, 3 ou 4) under budget and components choice constraints is proposed.

MOTS-CLÉS : Systèmes Instrumentés de Sécurité, Niveaux d'Intégrité de Sécurité, blocs diagrammes de fiabilité, allocation de disponibilité, allocation de redondance.

KEYWORDS: Safety Instrumented Systems, Safety Integrity Levels, reliability blocs diagrams, availability allocation, redundancy allocation.

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 (IEC61508, 1998) et l'IEC 61511 (IEC61511, 2000).

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 (Goble, 2006 ;Sallak, 2007). 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 et de réparation 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.* (1977) et Tzafestas (1980) ont publié des états de l'art sur les techniques d'optimisation de la fiabilité des systèmes. Dhillon (1986) et Misra (1986) ont proposé une liste de références sur l'allocation de la fiabilité. Récemment, Kuo *et al.* (2001) ont réactualisé l'ouvrage de Tillman *et al.* (1980). Yalaoui *et al. (2003)* 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.* (1999) 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.* (2003) ont également présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de maintenance. Elegbede *et al.* (2003) 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.

L'étude que nous proposons s'inscrit dans le contexte de l'allocation conjointe de la disponibilité et de la redondance des SIS. La méthodologie proposée est basée sur la modélisation fonctionnelle des systèmes par des structures séries parallèles sous forme de blocs diagrammes 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 (Lin, 1992 ; Painton *et al.,* 1995 ; Coit *et al.*, 1996 ; Elegbede *et al*., 1999, 2000 ; Yang, 1999).

A notre connaissance, le problème d'allocation de disponibilité et de redondance dans la conception des SIS pour le respect des allocations de SIL exigés 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 (IEC61508, 1998) et IEC 61511 (IEC61511, 2000).

La section 2 présente la procédure proposée par les normes IEC 61508 (IEC61508, 1998) et IEC 61511 (IEC61511, 2000) pour l'évaluation de la

disponibilité des SIS et l'allocation de SIL. La section 3 donne les notions de base de l'étude de disponibilité des systèmes réparables. La section 4 formule le problème d'allocation conjointe de disponibilité et de redondance des SIS. La section 5 illustre l'algorithme génétique utilisé dans la méthodologie proposée. La section 6 donne les paramètres de l'AG retenus. Dans la section 7, les résultats obtenus à l'aide de notre approche sont donnés et commentés. 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 (IEC61511, 2000) et IEC 61508 (IEC61508, 1998).

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 (cf. Figure 1) :

- 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.

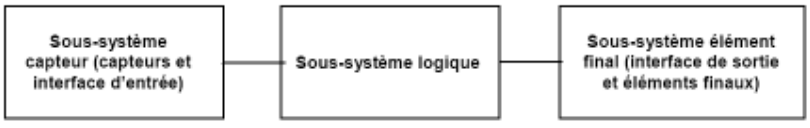

Figure 1. *Structure générale d'un Système Instrumenté de Sécurité*

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 (IEC61508, 1998) 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 (IEC61511, 2000) 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 (IEC61508, 1998) 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. Un des intérêts de cette norme est d'être générique et donc d'être applicable dans tous les secteurs où la sécurité peut être traitée avec des systèmes E/E/PE : industries manufacturières, industries des processus continus, pharmaceutiques, nucléaire, ferroviaire, etc.

2.2.2. *Norme IEC 61511*

La norme IEC 61511 (IEC61511, 2000) 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. Cette norme est spécifique à la production industrielle par processus dans le cadre de l'IEC 61508. Nous pouvons ainsi conclure que l'IEC 61511 est destinée aux intégrateurs et aux utilisateurs, alors que l'IEC 61508 reste une norme générique difficile à mettre en œuvre et dont les fabricants et les fournisseurs de systèmes E/E/PE se la sont appropriée.

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

La norme IEC 61508 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.

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. Optimisation de la disponibilité des systèmes réparables

Il existe deux moyens pour augmenter la disponibilité des systèmes réparables. La première est d'augmenter la disponibilité de chaque composant du système, en diminuant son taux de défaillance et/ou en augmentant son taux de réparation. La seconde approche est d'introduire des composants ou des sous-systèmes redondants. Or, l'ajout de composants en redondance augmente le coût total du système. C'est pourquoi une stratégie d'optimisation est nécessaire pour optimiser le coût et l'allocation conjointe de disponibilité et de redondance du système.

3.1. *Disponibilité des systèmes à composant unique*

Contrairement à la fiabilité qui s'intéresse au bon fonctionnement du système sur un intervalle de temps, [0, *t*], la disponibilité s'intéresse au bon fonctionnement à l'instant *t*, indépendamment du fait que le système ait pu avoir une ou plusieurs défaillances avant *t*. Elle prend en compte à la fois la fiabilité *R(t)* et la maintenabilité *M(t)* du système réparable.

3.1.1. *Disponibilité instantanée*

La disponibilité instantanée *A(t)* est l'aptitude d'une entité à être en état d'accomplir une fonction requise dans des conditions données, à un instant *t* donné, en supposant que la fourniture des moyens extérieurs nécessaires (notamment de maintenance et de détection immédiate) soit assurée :

A(t) = P (entité non défaillante à *t*)

Si nous considérons le cas où les taux de défaillance et de réparation des composants sont constants, alors la disponibilité instantanée d'un composant est exprimée par :

$$A(t) = \frac{1}{\mu + \lambda}(\mu + \lambda.e^{-(\lambda+\mu)t}) \quad [1]$$

3.2. *Disponibilité des systèmes multi composants*

Un système étant composé d'un ensemble de composants, la disponibilité instantanée du système s'écrit à partir de la disponibilité instantanée de ses composants selon l'architecture étudiée.

3.2.1. *Système série*

Si la défaillance d'un élément entraîne la défaillance du système, et si les défaillances sont indépendantes, l'ensemble est dit en série. A partir de l'équation [1], la disponibilité moyenne résultante vaut :

$$A(t) = \prod_i A_i(t) \quad [2]$$

Où $A_i(t)$ désigne la disponibilité instantanée du composant *i* à l'instant *t*.

3.2.2. *Système parallèle*

S'il suffit que l'un des éléments fonctionne pour que le système fonctionne, alors l'ensemble est dit en parallèle. La disponibilité moyenne résultante vaut :

$$A(t) = 1 - \prod_i (1 - A_i(t)) \quad [3]$$

3.2.3. *Système série-parallèle*

Pour un système représenté par une structure série parallèle (cf. Figure 2), en utilisant les équations [2] et [3], la disponibilité moyenne résultante vaut :

$$A(t)=\prod_j(1-\prod_i(1-A_i(t))=\prod_j(1-\prod_i(1-\frac{1}{\mu_i+\lambda_i}(\mu_i+\lambda_i e^{-(\lambda i+\mu i)t}))) \quad [4]$$

λ_i et μ_i désignent respectivement le taux de défaillance et le taux de réparation du composant i du sous-système j. Nous supposons ici que les composants redondants de chaque étage sont du même type.

3.3. *Disponibilité des SIS*

En utilisant l'équation [1], nous calculons la disponibilité instantané $A_i(t)$ de chaque composant i à l'instant t. La disponibilité instantanée $A(t)$ du SIS est ensuite calculée en utilisant l'équation [4]. Finalement, nous obtenons la disponibilité moyenne A_{avg} du SIS sur la période d'étude T par l'équation suivante :

$$A_{avg} = \frac{1}{T}\int_0^T A(t)\,dt \qquad \textbf{[5]}$$

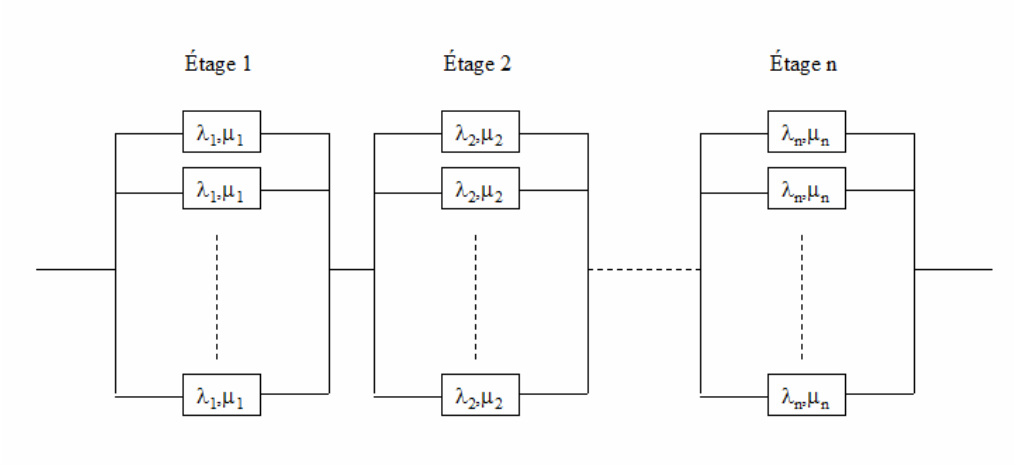

Figure 2. *Bloc diagramme de fiabilité d'un système série parallèle*

4. Algorithme génétique

4.1. *Introduction*

Nous sommes en présence d'un problème d'optimisation mono objectif (obtention du coût minimal) non continue sous plusieurs contraintes (disponibilité moyenne, coût maximal et nombre de composants disponibles). Pour résoudre ce type de problème, il existe diverses méthodes, qui se divisent principalement en deux

catégories : les méthodes déterministes et les méthodes stochastiques. Les techniques stochastiques tournent principalement autour des algorithmes stochastiques d'évolution de populations (algorithmes génétiques (AG), recuit simulé, etc.), qui sont des méthodes d'optimisation globale. Elles sont robustes, parallélisables et permettent de déterminer l'optimum global d'une fonctionnelle. Leur inconvénient majeur réside dans le nombre important d'évaluations nécessaires pour obtenir l'optimum recherché. Les méthodes déterministes de type gradient présentent en revanche l'avantage de converger rapidement vers un optimum. Cependant, elles ne sont pas aussi robustes que les techniques stochastiques et dépendent beaucoup du point de départ de recherche de l'extremum (Rao, 1996).

Dans cet article, nous proposons l'utilisation des AG pour les raisons suivantes :

- La mise en oeuvre des AG ne nécessite aucune hypothèse sur les paramètres du 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.
- Les AG permettent un équilibre entre exploitation et exploration (Beasley *et al.*, 1993). 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.
- Les AG ont montré de très bonnes performances dans la résolution de problèmes d'allocation de fiabilité et de redondance sur lesquels peu d'informations sont disponibles ou, pour lesquels il faut considérer de multiples critères d'optimisation (Kuo *et al*., 2000).

L'utilisation des AG pour l'allocation conjointe de disponibilité et de redondance parait donc évidente.

4.2. *Concepts de base*

Un AG est un algorithme itératif de recherche d'optimum, il manipule une population de taille constante (Holland, 1975 ; Goldberg, 1994). Cette population est formée de points candidats appelés chromosomes. La taille constante de la population entraîne un phénomène de compétition entre les chromosomes. Chaque chromosome représente le codage d'une solution potentielle au problème à résoudre. Un chromosome est constitué d'un ensemble d'éléments appelés gènes, pouvant prendre plusieurs valeurs appartenant à un alphabet non forcément numérique (Ludovic, 1994). A chaque itération, appelée génération, est créée une nouvelle population avec le même nombre de chromosomes. Cette génération consiste en des chromosomes mieux adaptés à leur environnement tel qu'il est représenté par la

fonction sélective. Au fur et à mesure des générations, les chromosomes vont tendre vers un optimum de la fonction sélective. La création d'une nouvelle population à partir de la précédente se fait par application des opérateurs génétiques que sont : la sélection, le croisement et la mutation (Renders, 1995). Ces opérateurs sont stochastiques. La sélection des meilleurs chromosomes est la première opération dans un AG. Au cours de cette opération l'algorithme sélectionne les éléments pertinents qui optimisent le mieux la fonction. Le croisement permet de générer deux nouveaux chromosomes, 2 enfants, à partir de deux chromosomes sélectionnés, parents, tandis que la mutation réalise l'inversion d'un ou plusieurs gènes d'un chromosome.

4.3. *Eléments de l'AG*

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

4.3.1. *Codage des solutions*

Dans un AG, nous ne travaillons pas directement avec les variables de décision du problème mais avec une représentation de celles-ci appelées codage. La forme codée d'une solution est une chaîne que nous appellerons chromosome. Ce chromosome est à son tour constitué d'éléments que nous appellerons gènes. Dans une population, nous parlerons indifféremment de chromosomes et d'individus. Dans la littérature, nous trouvons deux types de codages, les codages en nombres réels et les codages binaires (Goldberg, 1994). Le codage que nous avons utilisé est un codage en valeurs réelles. Dans ce type de codage, les gènes sont directement les valeurs recherchées. Dans cet article, les chromosomes sont définis comme étant des chaînes codant le nombre de composants en redondance dans chaque sous système du système.

4.3.2. *Population initiale*

Une fois le codage choisi, une population initiale formée de solutions possibles du problème (chromosomes) doit être déterminée. Plusieurs mécanismes de génération de la population initiale sont utilisés dans la littérature (Caux *et al.*, 1995). La population initiale peut être générée aléatoirement, par duplication et évolution ou en s'appuyant sur une heuristique.

4.3.3. *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 mais favoriseront la détermination de l'optimum.

4.3.4. *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. Ceci permet de donner aux individus dont la valeur de la fonction objectif est plus grande une probabilité plus élevée de contribuer à la génération suivante. Vladimir (1996) a démontré que lorsqu'un AG est utilisé pour maximiser une fonction objectif, alors c'est le processus de sélection qui assure la convergence vers un optimum global. Il existe plusieurs types de sélection (Goldberg, 1994). La technique de sélection la plus répandue est la technique du tournoi binaire stochastique 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 nous avons de parents géniteurs à sélectionner.

4.3.5. *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. Dans la littérature, plusieurs techniques de croisement sont utilisées dont les principaux sont le croisement barycentrique et le croisement à un ou plusieurs points (Goldberg, 1994 ; Michalewicz 1996 ; Back, 1995).

4.3.6. *Mutation*

L'opérateur de mutation permet d'introduire un facteur aléatoire dans les solutions générées, et d'élargir ainsi l'espace des solutions explorées (Koza, 1992 ; Goldberg, 1994 ; Michalewicz 1996) 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, nous choisissons une faible probabilité de mutation. Cette probabilité de mutation représente la fréquence à laquelle les gènes d'un chromosome sont mutés.

4.4. *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 …) qui gouvernent l'exploration des solutions,

mais aussi des conditions initiales. Il n'y a pas de règle générale pour le choix de ces paramètres. Chen *et al.* (1999) ont suggéré d'exécuter l'AG plusieurs fois avec différentes tailles de population, différentes valeurs de probabilités de croisement et de mutation afin de trouver l'ensemble des paramètres qui conviennent le plus au problème à optimiser. Nous avons réglé les paramètres de notre algorithme en suivant cette approche. Ainsi, après avoir exécuté 150 fois l'algorithme génétique et évalué l'impact du choix de chaque paramètre sur la convergence vers la solution optimale, nous obtenons les paramètres que nous allons utilisés dans la suite de notre problème.

5. 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 (2002) relatif à la norme IEC 61508. Ce SIS doit satisfaire à un SIL *i* (*i*=1, 2, 3 ou 4) exigé avec un coût de conception minimal et un choix réduit de composants.

5.1 *Présentation du système*

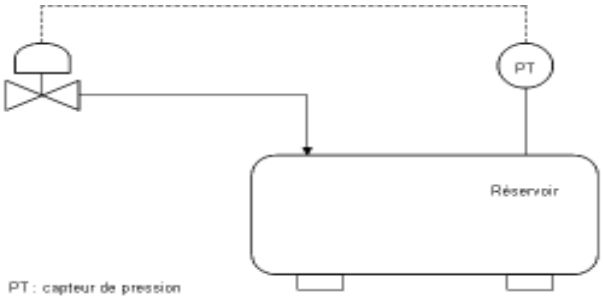

Figure 3. *Réservoir sous pression*

Nous considérons un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil (cf. Figure 3) (ISA, 2002). 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}. Pour montrer l'efficacité de la méthode, nous l'appliquons à plusieurs SIL exigés.

5.2. *Formulation du problème*

5.2.1. *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.

5.2.2. *Interprétation des objectifs*

Nous désirons avoir un niveau de SIL i (i=1, 2, 3 ou 4) avec un coût total minimal. Selon le Tableau 1, nous obtenons par exemple pour le SIL1 la contrainte suivante :

$$SIL1 \rightarrow 0.90 \leq A_{avg} \leq 0.99$$

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 i avec un coût total C_S minimal et ne dépassant pas C_{max}. C'est à dire qu'il faut trouver les n_C, n_U, n_a afin de :

Minimiser C_S [6]

Sous les contraintes :

- $A_{avg\min} \leq A_{avg} \leq A_{avg\max}$
- $C_S \leq C_{\max}$
- $n_{C\min} \leq n_C \leq n_{C\max}$
- $n_{U\min} \leq n_U \leq n_{U\max}$
- $n_{a\min} \leq n_a \leq n_{a\max}$

Où :

$$A_{avg} = \frac{1}{T}\int_0^T \prod_j (1 - \prod_i (1 - \frac{1}{\mu_i + \lambda_i}(\mu_i + \lambda_i . e^{-(\lambda_i + \mu_i)t}))dt$$

Symbole	Signification
S_i	Sous-système i
Cp_i	Capteur i
UT_i	Unité de traitement i
A_i	Actionneur i
n_C	Nombre de capteurs disponibles
n_U	Nombre d'unités de traitement disponibles
n_a	Nombre d'actionneurs disponibles
λ_{CPi}	Taux de défaillance du capteur i
λ_{UTi}	Taux de défaillance de l'unité de traitement i
λ_{Ai}	Taux de défaillance de l'actionneur i
μ_{CPi}	Taux de réparation du capteur i
μ_{UTi}	Taux de réparation de l'unité de traitement i
μ_{Ai}	Taux de réparation de l'actionneur i
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 et de réparation ainsi que le nombre de composants disponibles pour chaque sous-système du SIS et le coût total maximal à ne pas dépasser. Les valeurs des données de fiabilité ainsi que le coût des composants sont conformes à ceux utilisées sur le marché (Goble and Cheddie, 2006). Les coûts des composants des sous systèmes capteurs, unités de traitement et actionneurs sont respectivement 182, 60 et 3466 euros. Les paramètres retenus de l'algorithme génétique sont donnés dans le tableau 4. Les programmes d'optimisation ont été écrits sous Matlab 7.1. La figure 4 montre le codage que nous avons choisi pour les chromosomes. Le Tableau 5 donne le nombre de composants en redondance obtenus pour chaque sous système du SIS selon le SIL exigé. Les figures 4 et 5 donnent les configurations obtenues pour l'obtention des SIL 1 et 4.

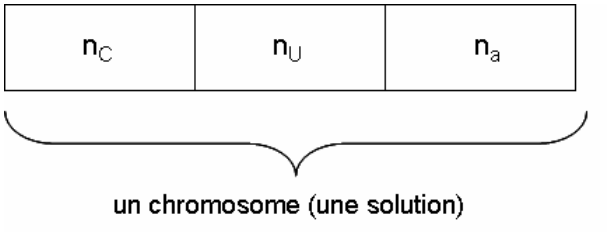

Figure 4. Codage d'une solution

Variables de décision	Valeurs
n_C	{2,3,…,20}
n_U	{2,3,…,20}
n_a	{2,3,…,20}
λ_{CPi}	9.10^{-3}
λ_{UTi}	9.10^{-3}
λ_{Ai}	5.10^{-3}
μ_{CPi}	8.10^{-3}
μ_{UTi}	$9.9\ 10^{-3}$
μ_{Ai}	8.10^{-3}
C_{max}	35000 euros

Tableau 3. *Valeurs des variables de décision*

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*

SIL	Nombre de Capteurs	Nombre d'Unités de traitements	Nombre d'Actionneurs	A_{avg}	C_s (euros)
1	8	8	3	0.9348	12300
2	11	11	5	0.9903	20000
3	14	11	8	0.99910	30900
4	10	11	16	0.99990	41800

Tableau 5. *Résultats obtenus pour chaque SIL exigé*

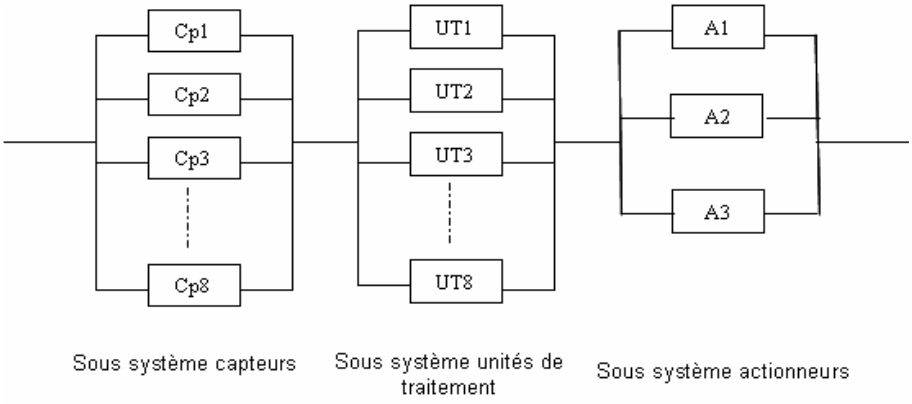

Figure 5. *Configuration pour une allocation SIL1 (A_{avg}= 0.9348, Cs=12300euros)*

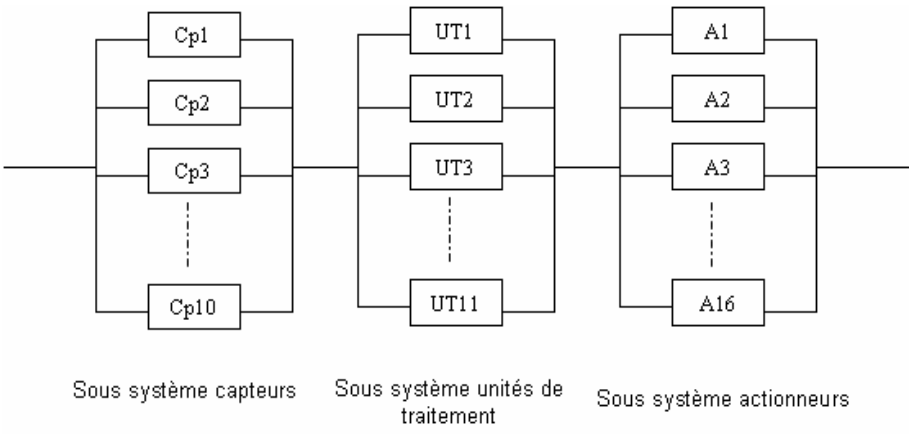

Figure 6. *Configuration pour une allocation SIL4 (A_{avg}=0.99990, Cs=41800 euros)*

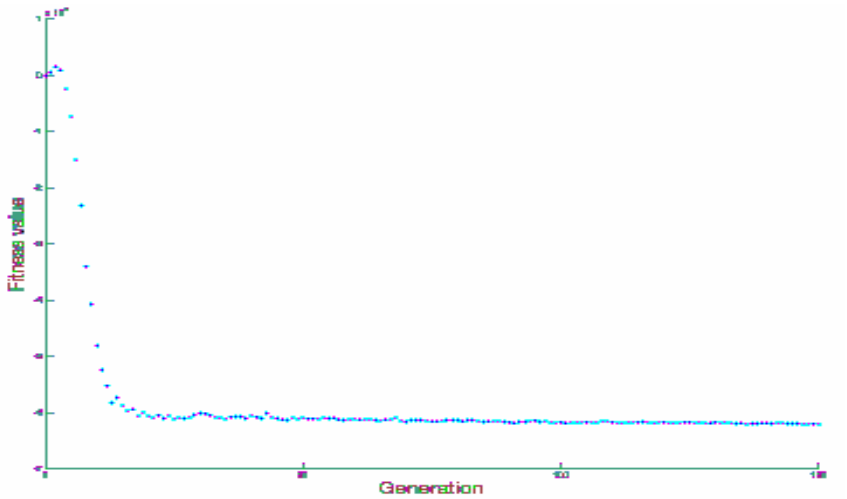

Figure 7. *Convergence de la fonction objectif pour l'obtention du SIL1*

5.3 Résultats

Les résultats obtenus peuvent être interprétés comme suit :

- Pour chaque SIL exigé, l'AG converge vers la solution optimale à partir de 115 générations. Dans la Figure 8, nous avons choisi de donner le tracé de la fonction objectif pour l'obtention du SIL1 en fonction du nombre de générations.

- Pour obtenir le SIL1 par exemple, le premier sous système contient 8 capteurs de taux de défaillance $\lambda = 9.10^{-3}$ et de taux de réparation $\mu = 8.10^{-3}$ placés en redondance, le deuxième sous système contient 8 unités de traitement de taux de défaillance $\lambda = 9.10^{-3}$ et de taux de réparation $\mu = 9.9.10^{-3}$ placées en redondance et le troisième sous système contient 3 actionneurs de taux de défaillance $\lambda = 5.10^{-3}$ et de taux de réparation $\mu = 8.10^{-3}$ placés en redondance (cf. Figure 5).
- Pour les SIL 1, 2 et 3, les configurations obtenues respectent les contraintes de coût. Ces trois configurations présentent des coûts inférieurs au coût maximum imposé (C_{max} = 35000 euros).
- Dans notre application, il n'existe pas de solutions permettant d'obtenir le SIL4 (cf. Figure 6), car nous devons dépasser le coût maximal imposé (C_s = 41800 > C_{max} = 35000 euros) pour obtenir une telle architecture.
- 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).
- Nous pouvons proposer comme solution la modélisation des SIS par des structures en couches complexes permettant tout type de connexion directe entre les composants des sous systèmes adjacents du SIS (cf. Figure 8).

6. Conclusion

Nous avons proposé une méthodologie d'allocation conjointe de disponibilité et de redondance des composants des SIS qui doivent satisfaire au niveau d'intégrité de sécurité (SIL) exigé par les normes de sécurité IEC 61508 et IEC 61511. Les résultats obtenus sont satisfaisants et les configurations obtenues qui sont données sous forme de blocs diagrammes de fiabilité respectent les contraintes imposées pour chaque SIL exigé.

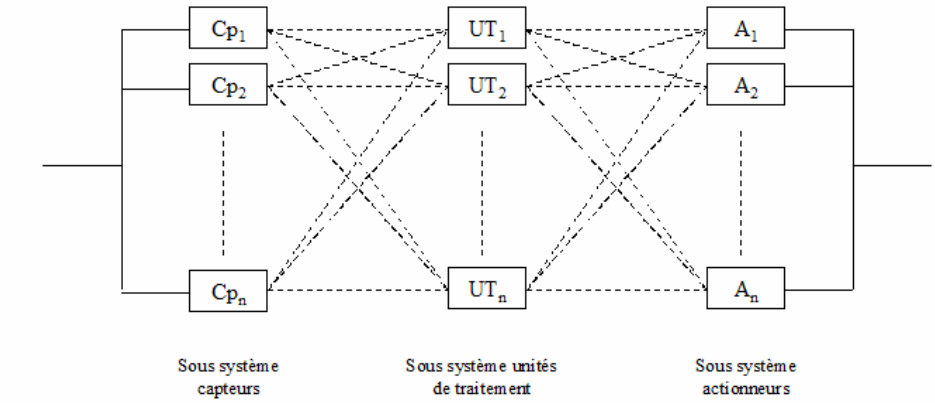

Figure 8. *Modélisation du SIS par une structure en couches complexe*

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 et de réparation des composants, mais aussi sur les politiques de maintenance préventives et correctives des SIS.

Nous travaillons actuellement sur la proposition d'une stratégie d'allocation de disponibilité des SIS non restreinte aux systèmes séries parallèles. Nous envisageons d'étendre nos travaux à différents types de configurations des SIS ayant des structures complexes en couches autorisant tout type de connexions et plus conformes aux SIS proposés actuellement sur le marché.

7. Bibliographie

Back T., *Evolutionary algorithms in theory and practice*, Oxford University Press, New-York, 1995.

Bhimavarapu K., Moore M., Stavrianidis P., « Performance based safety standards: an integrated risk assessment program », *ISA TECH*, vol. 1, 1997.

Castro H.P., Cavalca K.L., « Availability optimization with genetic algorithm », *International Journal of Quality and Reliability Management*, vol. 20, 2003, p. 847-863.

Chen J., Antipov E., Lemieux B., Cedeno W., Wood D. H., DNA computing implementing genetic algorithms. In L. F. Landweber, E. Winfree, R. Lipton, and S. Freeland, editors, Evolution as Computation, 1999, p. 39-49, New York. Springer Verlag.

Coit D.W., Smith A.E., « Reliability optimization of series-parallel systems using a genetic algorithm », *IEEE Transactions on Reliability*, vol. 45, n° 1, 1996, p. 254–260.

Dhillon B.I., « Reliability apportionment/allocation: a survey », *Microelectronics and Reliability*, 1986, vol. 26, p. 1121-1129.

Elegbede C., Adjallah K., « Reliability allocation to components following Weibull law using genetics algorithms », *ESREL'99*, *European Safety and reliability Conference*, Germany, 1999, p. 999-1004.

Elegbede C., Contribution aux méthodes d'allocation d'exigences de fiabilité aux composants de systèmes, Thèse de doctorat, Université de Technologie de Compiègne, 2000.

Elegbede C., Adjallah K., « Availability allocation to repairable systems with genetic algorithms: a multi-objective formulation », *Reliability Engineering and System Safety*, vol. 82, 2003, p.319-330.

Fletcher R., « An ideal penalty function for constrained optimization », *Journal of Applied Mathematics*, vol. 15, 1975, p. 319-342.

Giannakoglou K.C., « Designing turbomachinery blades using evolutionary methods », ASME Turbo Expo, Indianapolis, 1999.

Goble W. M., Cheddie H., Safety Instrumented Sytems Verification- Practical Probabilistic Calculations. ISA, 2006.

Goldberg D., Algorithmes génétiques, Addisson-Wesley, France, 1994.

Gomez S., Solano J., Castellanos L., Quintana M.I., Tunneling and genetic algorithm for global optimization, University of Mexico, 2000.

Holland J. H., *Adaptation in natural and artificial systems*, University of Michigan press, 1975.

IEC 61508. Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems, International Electrotechnical Commission (IEC), 1998.

IEC 61511. Functional safety: Safety Instrumented Systems for the process industry sector. International Electrotechnical Commission (IEC), 2000.

ISA-TR84.00.02-2002. Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation Techniques, Instrumentation Society of America (ISA), 2002.

Kim J.-H., Myung H., « Evolutionary programming techniques for constrained optimization problems », *IEEE Transactions on Evolutionary Comput*ation, vol. 1, n° 2, 1997, p. 129-140.

Koza J.R., *Genetic Programming: On the programming of computers by means of natural selection,* MIT Press, 1992.

Kuo W., Prasad V.R, Tillman F.A., Hwang C.L., *Optimal Reliability Design: Fundamentals and applications*, Cambridge, University Press, 2001.

Levitin G., Lisnianski A., « Joint redundancy and maintenance optimization for multi-state series-parallel systems », *Reliability Engineering and System Safety*, vol. 64, 1999, p. 33-42.

Lin C.Y., Hajela P., « Genetic algorithms in optimization problems with discrete and integer design variables », *Engineering Optimization*, vol. 19, 1992, p. 309-327.

Ludovic M., Audit de sécurité par algorithmes génétiques, Thèse de Doctorat, Université de Rennes 1, 1994.

Lutton E., Algorithmes génétiques et Fractales, Habilitation à diriger des recherches, Université Paris XI Orsay, 1999.

Marco B.N., Désidéri J.A., *Numerical solution of optimization test-cases by genetic algorithms*, Rapport de recherche INRIA Sophia Antipolis, vol. 3622, 1999.

Michalewicz Z., « A Survey of constraint handling techniques in evolutionary computation methods », *Proceedings of the 4th Annual Conference on Evolutionary Programming*, MIT Press, Cambridge, MA, 1995, p. 135-155.

Michalewicz Z., *Genetics Algorithms + Data Structures = Evolution Programs*, 3rd revised extended edition, Springer, 1996.

Misra K., « On optimal reliability design: a review », *System Science,* 1986, vol. 12, p. 5-30.

Ouaazizi A.E., Benslimane R., « Line fitting in noisy data using genetic algorithm », *3ème Conférence Internationale sur le Contrôle Qualité par Vision Artificielle QCAV'97*, 1997, p. 214-217.

Painton L., Campbell J., « Genetic algorithm in optimization of system reliability », *IEEE Transactions on Reliability,* vol. 44, 1995, p. 172-180.

Rao S.S., *Engineering optimization-theory and practice*, 3rd edition. New York: John Wiley & Sons, 1996.

Renders J.M., *Algorithmes génétiques et Réseaux de Neurones*, Editions HERMES, 1995.

Renders J.M., Flasse S.P., « Hybrid methods using genetic algorithms for global optimization», *IEEE Transactions on systems, man and cybernetics*, vol. 26, 1996, p. 243-258.

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.

Stavrianidis P., Bhimavarapu K., « Safety Instrumented Functions and Safety Integrity Levels (SIL) », *ISA Transactions*, 1998, vol. 37, p. 337-351.

Tillman F.A., Hwang C.L., Kuo W., « Optimization techniques for systems reliability with redundancy », *IEEE Transactions on Reliability*, 1977, vol. 26, p. 148-155.

Tillman F.A., Hwang C.L., Kuo W., *Optimization of systems reliability*, Marcel Dekker, NY., 1980.

Tzafestas S.G., « Optimization of system reliability: A survey of problems and techniques », *International Journal System Science*, 1980, vol. 11, p. 455-486.

Vicini A., Quagliarella D., « Airfoil and wing design through hybrid optimization strategies», *AIAA*, 1998, p. 27-29.

Yalaoui A., Chu C., Chatelet E., « Allocation de fiabilité et de redondance. Les systèmes parallèle-série», Journal Européen des Systèmes Automatisés (Jesa), vol. 38, 2004, p.85-102.

Yang J-E., Hwang M-J., Sung T-Y., Jin Y., « Application of genetic algorithm for reliability allocation in nuclear power plants », *Reliability Engineering and System Safety*, vol. 65, 1999, p. 229-238.