Conception optimale des systèmes instrumentés de sécurité : une approche par les blocs diagrammes de fiabilité

Mohamed Sallak, Christophe Simon, Jean-François Aubry

CONCEPTION OPTIMALE DES SYSTEMES INSTRUMENTÉS DE SECURITÉ : UNE APPROCHE PAR LES BLOCS DIAGRAMMES DE FIABILITÉ

M. Sallak, J.-F. Aubry

CRAN-UMR 7039,
Nancy University, CNRS,
ENSEM, 2 Avenue de la forêt de Haye
54506 Vandoeuvre-Les-Nancy
mohamed.sallak@ensem.inpl-nancy.fr
jean-francois.aubry@isi.u-nancy.fr

C. Simon

CRAN-UMR 7039,
Nancy University, CNRS,
ESSTIN, 2 Rue Jean Lamour
54519 Vandoeuvre-Les-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 la disponibilité et de la redondance des SIS. Elle est basée sur la modélisation des SIS par des systèmes séries parallèles sous forme de blocs diagrammes de fiabilité. La méthode d'optimisation choisie est les algorithmes génétiques. En guise d'illustration, la méthodologie est appliquée à la conception d'un SIS, utilisé dans le document ISA-TR84.00.02-2002 relatif à la norme IEC 61508, qui doit implémenter une Fonction Instrumentée de Sécurité de SIL 1 avec un coût minimal et un choix réduit de composants. L'architecture obtenue qui est donnée sous forme d'un bloc diagramme de fiabilité respecte le niveau de SIL exigé et le coût de conception maximal.*

MOTS-CLÉS : *Systèmes Instrumentés de Sécurité, niveau d'Intégrité de Sécurité, conception optimale, disponibilité, blocs diagrammes de fiabilité, algorithmes génétiques*

1. INTRODUCTION

Lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont mises en oeuvre. 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, deux normes de sécurité sont utilisées : l'IEC 61508 (IEC61508, 1998) et l'IEC 61511 (IEC61511, 2000).

Cependant, les fiabilistes ont beaucoup de difficultés à mettre en œuvre les prescriptions de ces deux normes pour la conception des SIS dont on exige un niveau d'Intégrité de Sécurité (SIL, Safety Integrity Level) donné. Le SIL exprime la réduction de risque qui doit être réalisée par le SIS. Il est certain qu'une stratégie de conception dont le souci est purement technique, permet d'atteindre le SIL exigé, mais elle le fait au détriment du coût de conception du SIS. Par contre, si la stratégie de conception cherche uniquement à réduire le coût de conception, le résultat est un nombre important de défaillances dangereuses et le non respect du SIL. En conséquent, il est devenu 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 des systèmes sont très nombreuses. Elles se différencient par de nombreux points tels que :

- Le paramètre à optimiser : fiabilité, disponibilité, maintenabilité, etc.
- Le type de système considéré : série, parallèle, série parallèle, etc.
- L'approche considérée : on distingue deux principales approches d'allocation. L'une est appelée approche par pondération où l'on part de l'objectif de sûreté de fonctionnement considéré et on cherche à le distribuer aux composants du système de telle sorte que l'objectif global soit atteint. La deuxième est appelée approche par

optimisation où l'on cherche une solution répondant à des critères d'optimalité en considérant les variables de décision (disponibilités des composants par exemple).

- L'algorithme d'optimisation : recuit simulé, recherche avec tabous, algorithmes génétiques, etc.

Pour prendre en compte les aspects de défaillance et de réparation des composants, on s'intéresse à l'allocation de disponibilité. En outre, pour prendre en compte le choix limité de composants disponibles sur le marché, on s'intéresse à l'allocation de redondance. Par conséquent, les travaux de cet article sont orientés vers une stratégie de conception optimale 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 aussi une liste de références sur l'allocation de la fiabilité. Récemment, Kuo et al. (2001) ont réactualisé l'ouvrage de Tillman et al. (1980). En ce qui concerne l'allocation conjointe de disponibilité et de redondance, très peu de travaux ont été réalisés. 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. 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. Castro et al. (2003) ont présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de maintenance.

L'étude qu'on propose 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 des systèmes par des systèmes séries parallèles sous forme de blocs diagrammes de fiabilité. La méthode d'optimisation choisie est les algorithmes génétiques. Le choix des algorithmes génétiques est motivé par le fait qu'on est en présence d'un problème d'optimisation avec une fonction objectif non continue. 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 tel que 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 el 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. Aussi, 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, afin de satisfaire au niveau de SIL exigé en conformité avec les normes de sécurité IEC 61508 (IEC61508, 1998) et IEC 61511 (IEC61511, 2000).

La section 2 présentera 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 donnera les notions de base de l'étude de disponibilité des systèmes réparables. La section 4 formulera le problème d'allocation de disponibilité et de redondance des SIS. La section 5 illustrera l'algorithme génétique utilisée dans la méthodologie proposée. La section 6 donnera et les paramètres de l'AG retenus. Dans la section 7, les résultats obtenus à l'aide de notre approche seront donnés et commentés. Enfin, nous conclurons avec les perspectives des travaux de cet article.

2. PROCEDURE POUR L'EVALUATION 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 en conformité avec les normes de sécurité IEC 61511 (IEC61511, 2000) et IEC 61508 (IEC, 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, etc.) 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

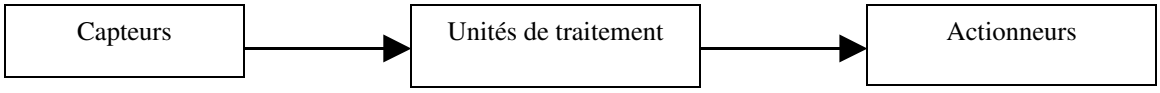

Figure 1. Structure générale d'un SIS

2.2. Référentiel normatif

La sécurité fonctionnelle a depuis longtemps retenu l'attention des industriels. Pour mener à bien leur démarche sécurité, ils peuvent s'appuyer sur des normes. La norme internationale de sécurité IEC 61508 (IEC, 1998) est une des dernières normes dédiées à la sécurité fonctionnelle. Les normes filles que cette norme de base a générées, comme l'IEC 61511 (IEC61511, 2000) applicable au secteur de l'industrie des procédés, sont plus récentes et restent encore assez peu connues des acteurs de la sécurité dans certains secteurs industriels français. 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 (IEC, 1998) est une norme internationale qui porte plus particulièrement sur les systèmes E/E/PE, c'est-à-dire les systèmes 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 process 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 oeuvre 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 est une norme générique difficile à mettre en oeuvre et donc destinée surtout aux fabricants et fournisseurs de systèmes E/E/PE.

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

La norme IEC 61508 (IEC61508, 1998) fixe le niveau d'Intégrité de Sécurité (SIL) qui doit être atteint par un SIS. Elle donne le SIL en fonction de la disponibilité moyenne A_{avg} pour les SIS faiblement sollicités (moins d'une sollicitation par an) (cf. Tableau 1) et en fonction du nombre de défaillances par heure (N) pour les SIS fortement sollicités ou agissant en mode continu (cf. Tableau 1). Dans cet article, nous nous intéressons 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. ALLOCATION DE DISPONIBILITÉ DES SYSTEMES REPARABLES

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 ou en augmentant son taux de réparation. Dans cette approche, il est clair qu'il faut prendre en compte aussi l'existence de composants sur le marché avec de tels taux de défaillance et 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.

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 (Availability) 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 (cf. Figure 2).

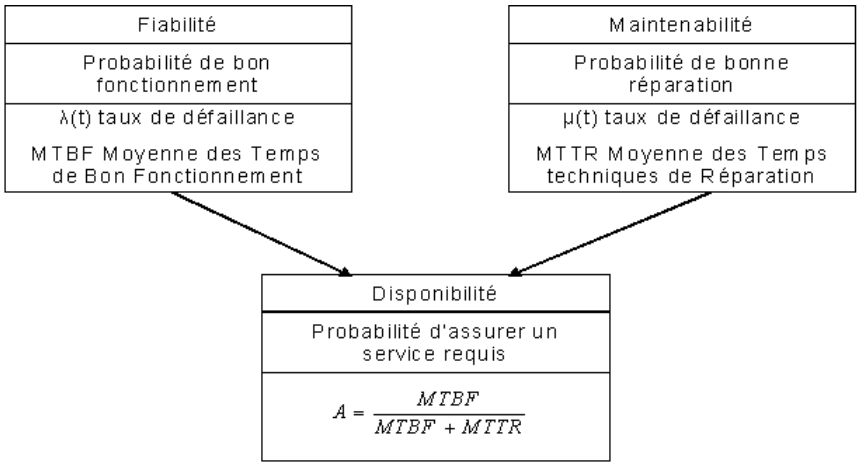

Figure 2. Fiabilité, maintenabilité et disponibilité d'un système réparable

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 soit assurée :

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

3.1.2 Disponibilité moyenne

La disponibilité moyenne, notée $\widetilde{A}(t)$, sur *[0, t]*, est exprimée par :

$$\widetilde{A}(t) = \frac{1}{t}\int_0^t A(x)dx \qquad (1)$$

3.1.3 Disponibilité moyenne limite

La disponibilité moyenne limite est la valeur limite de l'expression [1] :

$$A = \lim_{t\to\infty} \frac{\int_0^t A(x)dx}{t} \qquad (2)$$

Lorsque les taux de défaillance λ et les taux de réparation μ sont constants (i.e. les lois de probabilité de *R(t)* et de *M(t)* sont exponentielles), alors le MTBF (moyenne des temps de bon fonctionnement) est l'inverse du taux de défaillance :

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

et le MTTR (moyenne des temps techniques de réparation) est l'inverse du taux de réparation :

$$MTTR = \frac{1}{\mu}$$

La disponibilité moyenne limite peut alors être exprimée par :

$$A = \frac{\mu}{\mu + \lambda} = \frac{MTBF}{MTTR + MTBF} \qquad (3)$$

3.2. Disponibilité des systèmes multi composants

3.2.1 Systèmes séries

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 la formule 3, la disponibilité moyenne résultante vaut :

$$A = \prod_i A_i = \prod_i \frac{\mu_i}{\lambda_i + \mu_i} \qquad (4)$$

3.2.2 Systèmes parallèles

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

$$A = 1 - \prod_i (1 - A_i) = 1 - \prod_i \frac{\lambda_i}{\lambda_i + \mu_i} \qquad (5)$$

3.2.3 Système séries parallèles

Pour un système redondant représenté par un système série parallèle (cf. Figure 3), en utilisant les formules 4 et 5, la disponibilité moyenne résultante vaut :

$$A = \prod_{i=1}^{s} (1 - (\frac{\lambda_i}{\lambda_i + \mu_i})^{k_i}) \qquad (6)$$

k_i : Nombre de composants redondants dans le sous-système *i*.

s : Nombre de sous-systèmes du système complet.

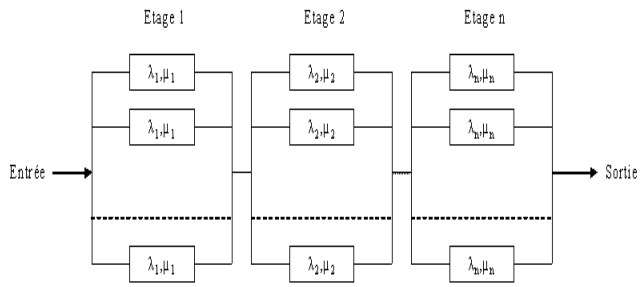

Figure 3. Bloc diagramme de fiabilité d'un système série parallèle

3.3. Coût des composants

Afin de relier le coût d'un composant avec sa fiabilité, les auteurs ont proposé différentes fonctions de coût. Parmi les fonctions les plus utilisées dans la littérature, citons par exemple les fonctions de Breipohl, Truelove, Misra et al. ou encore de Tillman et al. (Elegbede, 2000). Pour de tenir compte des aspects de défaillance et de réparation des SIS et de leur répercutions sur le coût total du SIS, dans cet article, on choisit une fonction coût qui prend en compte la disponibilité du système, et donc qui dépend de λ et μ (Elegbede, 2003) :

$$C = \sum_{i=1}^{s} k_i (a_i \lambda_i^{pi} + b_i \mu_i^{qi}) \quad (7)$$

où a_i, b_i, p_i et q_i sont des nombres réels convenablement choisis tels que : $a_i > 0$, $b_i > 0$, $p_i < 0$ et $q_i > 0$ (i=1,2,…,s). Ces paramètres sont en général choisis par les fiabilistes qui ont la charge de surveiller le système étudié.

4. FORMULATION DU PROBLEME

On considère un système constitué d'un réservoir sous pression contenant un liquide inflammable volatil (cf. Figure 4) (ISA-TR84.00.02-2002, 2002). Ce réservoir peut rejeter des gaz dans l'atmosphère.

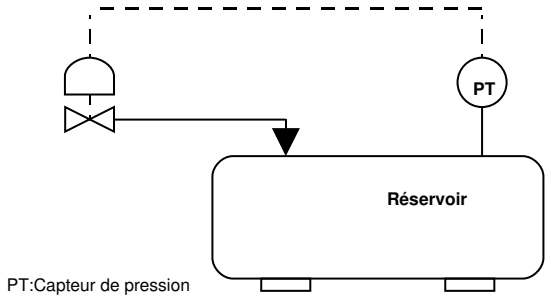

Figure 4. Réservoir sous pression

On suppose 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 de niveau SIL 1 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 de SIL 1, avec un coût total minimal qui ne dépasse pas 110 unités. On choisit de représenter le fonctionnement du SIS par un diagramme de fiabilité représenté sur la Figure 4. Le SIS est constitué de trois sous système :

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

Chaque sous système peut contenir un ou plusieurs composants du même type de composants en parallèles.

4.1. Notations

Pour formuler le problème de l'allocation de redondance et de disponibilité du SIS, nous allons utiliser les notations données dans le tableau 2.

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_s	Fiabilité du SIS
C_s	Coût total du SIS

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

4.2. Interprétation des objectifs

On désire avoir un niveau de SIL 1 et puisque on travaille avec des SIS faiblement sollicités, donc selon le tableau 1, on obtient :

$$SIL1 \quad 0.90 \quad A_{avg} \quad 0.99$$

Pour chaque sous-système *i* on une contrainte en plus, qui est le nombre de composants disponibles, les bornes du taux de défaillance et les bornes du taux de réparation de chaque composant. On cherche le nombre de composants utilisés dans chaque sous-système i afin d'obtenir la fonction instrumentée de sécurité de SIL 1 avec une disponibilité maximale et un coût total minimal et ne dépassant pas 110 unités. C'est à dire :

Trouver les n_C, n_U, n_a afin de (i=1,2,3) :

Minimiser C_S (8)

Sous les contraintes :

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

$$C_S \blacksquare C_{\max}$$

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

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

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

Où : $A_{avg} = \prod^{3} (1-(\frac{\lambda_i}{\lambda_i+\mu_i})^{k_i})$

$$C_S = \sum^{3} k_i(a_i\lambda_i^{pi} + b_i\mu_i^{qi})$$

5. ALGORITHME GENETIQUE (AG)

5.1. Introduction

D'après la formulation de [8], on déduit que c'est un problème d'optimisation mono objective non linéaire avec plusieurs contraintes. 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,…), 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 (Rao, 1996).

Développés par Holland (1975) 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) (Goldberg, 1994 ; Lutton, 1999).

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 (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.
- La troisième raison est que les AG ont montré de très bonnes performances dans la résolution de problèmes d'allocation de fiabilité et de redondance sur lesquels peu d'informations sont disponibles ou pour lesquels il faut considérer de multiples critères d'optimisation (Kuo et al., 2000).

5.2. Concepts de base

Un AG est un algorithme itératif de recherche d'optimum, il manipule une population de taille constante. 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, il est constitué d'un ensemble d'éléments appelés gènes, pouvant prendre plusieurs valeurs appartenant à un alphabet non forcément numérique (Ludovic, 1994). A chaque itéra-

tion, 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 l'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 mieux la fonction. Le croisement permet de générer deux chromosomes nouveaux « enfants » à partir de deux chromosomes sélectionnés « parents », tandis que la mutation réalise l'inversion d'un ou plusieurs gènes d'un chromosome.

5.3. Opérateurs 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. Dans une population, on parlera indifféremment de chromosomes et d'individus. Dans la littérature, on trouve 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. 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. La population initiale peut être générée aléatoirement, par duplication et évolution ou en s'appuyant sur une heuristique (Caux et al., 1995). 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. Vladimir (1996) a démontré que lorsqu'un AG est utilisé pour maximiser une fonction objective, alors c'est le processus de sélection qui assure la convergence vers un optimum global. Il existe plusieurs types de sélection (Goldberg, 1994). 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.

5.3.4 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). 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.

5.3.5 Mutation

L'opérateur de mutation permet d'introduire un facteur aléatoire dans les solutions générées, et d'élargir ainsi l'espace des solutions explorées (Goldberg, 1994 ; Michalewicz 1996 ; Koza, 1992) 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 chro-

mosome et à le remplacer par une valeur aléatoire avec une probabilité de mutation P_m=*0.03*.

6. CHOIX DES PARAMETRES 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, Woods (1997) a suggéré de l'exécuter plusieurs fois avec différentes tailles de population, probabilités de croisement et de mutation afin de trouver l'ensemble des paramètres qui conviennent le plus à l'utilisateur. C'est cette méthode qu'on a choisie. Après avoir exécuté 150 fois notre AG, on obtient les paramètres donnés dans le tableau 3.

7. APPLICATION NUMERIQUE

On considère le SIS qui est présenté dans la section 4 (cf. Figure 4). Le tableau 4 présente les valeurs des taux de défaillance et de réparation ainsi que les nombres maximum et minimum de composants disponibles pour chaque sous-système du SIS. L'objectif étant d'obtenir le SIL 1 tout en minimisant le coût des composants utilisés et ne pas dépasser un coût de 110 unités. Les paramètres de l'algorithme génétique sont donnés dans le tableau 3. Les résultats obtenus par la méthode d'optimisation proposée sont illustrés dans le tableau 5 et la Figure 5.

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 3. Paramétrage de l'algorithme génétique

Variables de décision	Valeurs maximales	Valeurs minimales	Coût (unités)
A_{avg}	0.90	0.99	-
n_C	2	10	-
n_U	2	5	-
n_a	2	10	-
λ_{CPi}	-	9.10^{-3}	13
λ_{UTi}	-	9.10^{-3}	13
λ_{Ai}	-	7.10^{-3}	11
μ_{CPi}	-	8.10^{-3}	11
μ_{UTi}	-	$9.9\ 10^{-3}$	12
μ_{Ai}	-	8.10^{-3}	12
C_S	110	-	

Tableau 4. Bornes des variables de décision

Sous-système	**Nombre de composants**	**Taux de défaillance**	**Taux de réparation**
1	2	0.009	0.008
2	3	0.009	0.0099
3	3	0.007	0.008

Tableau 5. Paramètres obtenus pour les variables de décisions

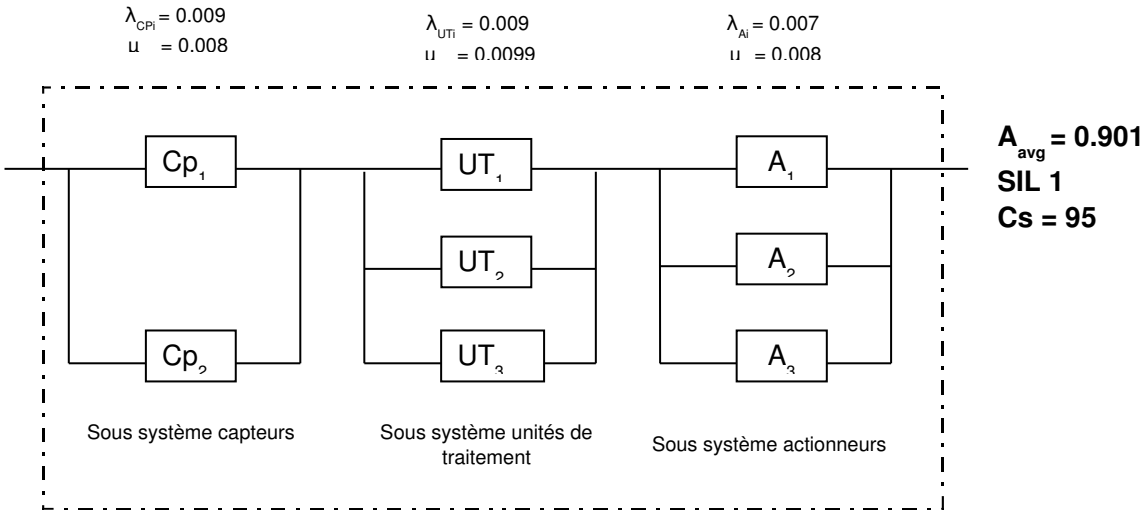

Figure 5. Configuration obtenue du SIS pour l'obtention du SIL 1

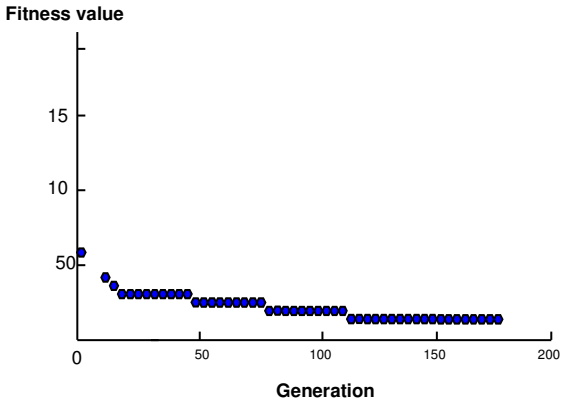

Figure 6. Convergence de la fonction objective en fonction du nombre de génération

Les résultats peuvent être interprétés comme suit :

- Les résultats fournis par l'AG sont cohérents avec les valeurs des données pour chaque paramètre.
- L'AG converge rapidement vers la solution optimale à partir de 115 générations (cf. Figure 6).
- La configuration obtenue respecte le SIL exigé et la contrainte de coût.
- Il est important de souligner que l'approche proposée ici peut être étendue aux systèmes du type *k* parmi *n* (le système fonctionne si *k* composants fonctionnent parmi *n composants*).

8. CONCLUSION

La méthodologie d'allocation de disponibilité et de redondance des SIS que nous avons proposée a pour objectif de satisfaire au niveau d'intégrité de sécurité (SIL) exigé par les normes de sécurité IEC 61508 (IEC 61508, 1998) et IEC 61511 (IEC 61511, 2000). On a modélisé le SIS par un système série parallèle sous forme de bloc diagramme de fiabilité afin d'obtenir une expression explicite de la disponibilité qui facilite le processus d'optimisation. Cette procédure d'optimisation utilise un algorithme génétique. Les résultats obtenus sont satisfaisants puisque nous avons obtenu des structures qui ont permis de satisfaire au niveau de SIL exigé avec un coût de conception minimal ne dépassement pas le coût maximal imposé.

Des paramètres additionnels peuvent être pris en considération au niveau du modèle. C'est ainsi qu'une stratégie optimale peut être obtenu en raisonnant non seulement sur les taux de défaillance et de réparation 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 ou du type *k* parmi *n*. Nous envisageons en effet, d'étendre nos travaux à différents types de configuration des SIS qui ont des structures complexes plus conformes aux SIS proposés actuellement dans le marché. Cette extension sera basée sur l'utilisation des réseaux de fiabilité au lien des blocs diagrammes de fiabilité. L'intérêt des réseaux de fiabilité est de pouvoir modéliser tout type de structure. Cependant, le calcul de la disponibilité d'un réseau de fiabilité et son insertion dans un processus d'optimisation ne sont pas aisé.

REFERENCES

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

Beasley D., D.R. Bull, and R.R. Martin, 1993. *An overview of genetic algorithms : Part 1, fundamentals*. University Computing, 15, p. 58-59.

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

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

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

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

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

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

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

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

IEC61508, 1998. *Functional safety of Electrical/Electronic/Programmable Electronic (E/E/PE) safety related systems*, International Electrotechnical Commission (IEC).

IEC61511, 2000. *Functional safety: Safety Instrumented Systems for the process industry sector.* International Electrotechnical Commission (IEC).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vladimir F., 2003. Fine-grained tournament selection operator in genetic algorithms. Computing and Informatics, 22, p. 143-162.

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