

Allocation de disponibilité et de redondance : Une approche par les réseaux de fiabilité

Mohamed SALLAK¹, Jean-Francois AUBRY¹, Christophe SIMON²

¹CRAN-UMR 7039, Nancy Université, CNRS
2, Avenue de la forêt de Haye
54506, Vandœuvre-les-Nancy, France

² CRAN-UMR 7039, Nancy Université, CNRS
2, Rue Jean Lamour
54519, Vandœuvre-les-Nancy, France

mohamed.sallak@ensem.inpl-nancy.fr, jean-Francois.aubry@isi.u-nancy.fr,
christophe.simon@esstin.uhp-nancy.fr

Résumé— Cet article propose une méthodologie d'allocation conjointe de disponibilité et de redondance des composants des systèmes. La méthodologie est basée sur l'utilisation des réseaux de fiabilité. La technique d'optimisation choisie est les algorithmes génétiques (AG). En guise d'illustration, la méthodologie est appliquée à la conception d'un Système Instrumenté de Sécurité (SIS) défini dans le document ISA-TR84.00.02-2002 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.

Mots-clés— réseaux de fiabilité, allocation de disponibilité et de redondance, Systèmes Instrumentés de Sécurité, Niveaux d'Intégrité de Sécurité, algorithmes génétiques.

I. INTRODUCTION

Aujourd'hui, il est devenu primordial de trouver une stratégie d'allocation de paramètres de sûreté de fonctionnement des composants des systèmes automatisés qui permet d'établir le meilleur compromis entre les exigences de sûreté de fonctionnement requises et le coût de conception de ces systèmes. 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, etc.
- Le type d'architecture considérée : série, parallèle, etc.
- L'approche considérée : soit une approche par pondération où nous partons de l'objectif de sûreté de fonctionnement considéré et nous cherchons à le distribuer aux composants de telle sorte que l'objectif global soit atteint. Soit une approche par optimisation où nous cherchons une solution répondant à des critères d'optimisation en considérant les variables de décision.
- L'algorithme d'optimisation :
 - Méthodes directes : gradients, programmation dynamique, etc.
 - Heuristiques et méta heuristiques : recuit simulé, recherche tabou, algorithmes génétiques, 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 prendre en compte

le 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. [1] et Tzafestas [2] ont publié des états de l'art sur les méthodes d'allocation de fiabilité. Dhillon [3] et Misra [4] ont proposé une liste de références sur l'allocation de la fiabilité. Récemment, Kuo et al. [5] ont réactualisé l'ouvrage de Tillman et al. [1]. En ce qui concerne l'allocation conjointe de disponibilité et de redondance, Levitin et al. [6] 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. [7] ont également présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de maintenance. Elegbede et al. [8] 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. A notre connaissance, le problème d'allocation de disponibilité et de redondance dans la conception des systèmes en utilisant les réseaux de fiabilité n'a pas été traité auparavant. En outre, la méthodologie sera appliquée à la conception d'un Système Instrumenté de Sécurité (SIS) défini dans le document ISA-TR84.00.02-2002 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.

La section 2 présente la procédure proposée par les normes IEC 61508 et IEC 61511 [9], [10] pour l'évaluation de la

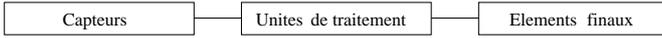


Fig. 1. Structure générale d'un Système Instrumenté de Sécurité

disponibilité des SIS et l'allocation de SIL. La section 3 introduit les notions de base de l'étude des réseaux de fiabilité. La section 4 illustre l'algorithme génétique utilisé. La section 5 formule le problème d'allocation de disponibilité et de redondance des SIS. Les résultats obtenus à l'aide de notre approche sont donnés et commentés. Enfin, nous concluons sur les perspectives de ce travail.

II. 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 et IEC 61508 [9], [10].

A. Systèmes Instrumentés de Sécurité (SIS)

Un SIS est un système visant à mettre le procédé en position de replis de sécurité, 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. Fig. 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.

B. 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 IEC 61508 [9] est une norme internationale qui porte plus particulièrement sur les systèmes E/E/PE (électriques/électroniques/électroniques programmables de sécurité). La norme IEC 61511 [10] permet de définir des exigences relatives aux spécifications, à la conception, à l'installation, à l'exploitation et à l'entretien d'un SIS. Cette norme est spécifique à la production industrielle par processus dans le cadre de l'IEC 61508.

C. 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 un SIS. Elle 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. Table 1). Dans cet article, nous nous intéressons uniquement à l'étude des SIS faiblement sollicités.

TABLE I
DÉFINITION DU NIVEAU DE SIL

SIL	Demande faible	Demande élevée
	PFH_{avg}	Défaillances/heure
1	$[10^{-2}, 10^{-1}]$	$[10^{-6}, 10^{-5}]$
2	$[10^{-3}, 10^{-2}]$	$[10^{-7}, 10^{-6}]$
3	$[10^{-4}, 10^{-3}]$	$[10^{-8}, 10^{-7}]$
4	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

III. RÉSEAUX DE FIABILITÉ

Dans cette section, nous allons présenter les réseaux de fiabilité tels qu'ils ont été défini par Kaufmann *et al.* [11].

A. 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 [11], [12], [13]. Considérons un ensemble fini S et le produit $S \times S$. Soit U un sous ensemble de $S \times S$. le couple :

$$G = (S, U)$$

est appelé un multigraphe (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.

B. Concepts de base des réseaux de fiabilité

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

- Un graphe r -appliqué $G = (S, U)$ sans boucles, dans lequel deux sommets $O \in S$ et $Z \in S$ sont distingués et appelés respectivement "origine" et "extrémité".
- Une application $\Delta : U \rightarrow e$ telle que :

$$\Omega(u_j) = (S_i, S_k), \quad \Omega(u_{j'}) = (S_i, S_k) \Rightarrow \Delta(u_j) \neq \Delta(u_{j'}) \quad (1)$$

où Ω est l'application qui fait correspondre à chaque arc le couple de ses extrémités.

L'application Δ fait correspondre à chaque arc du graphe un composant. Plusieurs arcs peuvent correspondre à un même composant (il se peut qu'un arc ne corresponde à aucun composant). La figure 2 donne un exemple de réseau de fiabilité où :

$$e = \{e_1, e_2, e_3, e_4\} \quad (2)$$

$$S = \{O, Z, A, B, C\} \quad (3)$$

$$U = \{OA_{e_2}, OA_{e_3}, OB, AB, AZ, BC, BZ, CB, ZB\} \quad (4)$$

L'application Δ est indiquée par les e_i affectés aux arcs.

C. Lien d'un réseau de fiabilité

A tout sous-ensemble de composants $e_i \subset e$, nous pouvons faire correspondre le graphe partiel $G_p(e_i)$ du graphe

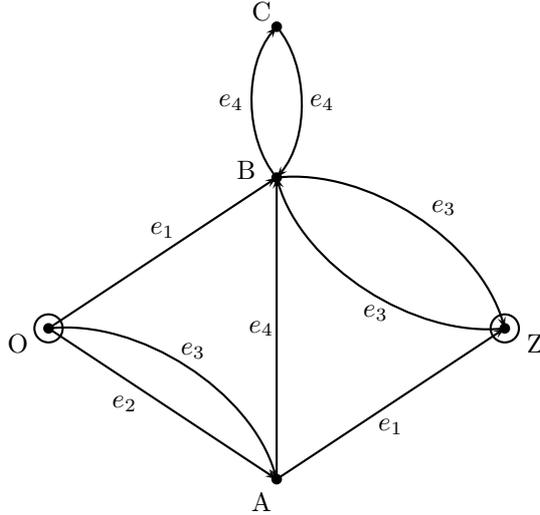


Fig. 2. Réseau de fiabilité

G , obtenu en ne conservant que les arcs de G auxquels correspond un composant appartenant à e_i :

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

avec :

$$U_p(e_i) = \{u \in U \mid \Delta(u) \in e_i\}. \quad (6)$$

Nous appellerons "lien" d'un réseau R un sous-ensemble de composants $a \subset e$ tel qu'il existe dans le graphe $G_p(a)$ un chemin de O à Z . Par exemple, $\{e_1, e_2, e_3\}$ est un lien du réseau de la figure 2. A tout lien correspondent un ou plusieurs chemins du graphe. Inversement, à un chemin $\mu = (u_1, u_2, \dots, u_l)$ de O à Z correspond le lien a formé des images des arcs u_1, u_2, \dots, u_l par l'application Δ . Par exemple, au chemin $\mu = ((OA)_{e_3}, AB, BZ)$ correspond le lien $a = \{e_3, e_4\}$.

D. Coupe d'un réseau de fiabilité

Nous appellerons "coupe" d'un réseau R un sous-ensemble de composants $b \subset e$ tel que le sous-ensemble d'arcs $U_p(b)$ contienne une coupe du graphe G relative à un sous-ensemble de sommets incluant Z et n'incluant pas O . Par exemple, $\{e_1, e_2, e_3\}$ est une coupe du réseau (en même temps qu'un lien) ; le sous-ensemble complémentaire $\{e_4\}$ n'est ni une coupe, ni un lien. A toute coupe b du réseau correspondent donc une ou plusieurs coupes du graphe incluses dans $U_p(b)$. Dans l'exemple ci-dessus, l'ensemble d'arcs $\{AZ, BZ\}$ est une coupe du graphe qui n'inclut pas les arcs OB , $(OA)_{e_2}$ et $(OA)_{e_3}$.

E. Lien minimal et coupe minimale d'un réseau de fiabilité

Un lien a est minimal si aucun sous-ensemble $a' \subset a$ n'est un lien du réseau. Une coupe b est minimale si aucun sous-ensemble $b' \subset b$ n'est une coupe du réseau. Dans la figure 2, $\{e_1, e_2, e_3\}$ n'est pas un lien minimal ; $\{e_1, e_3\}$ en est un, c'est également une coupe minimale. $\{e_1, e_4\}$ est un autre exemple de coupe minimale.

Un réseau de fiabilité n'est pas un schéma de connexion physique des éléments mais seulement un modèle formelle du comportement dysfonctionnel ; si nous connais-

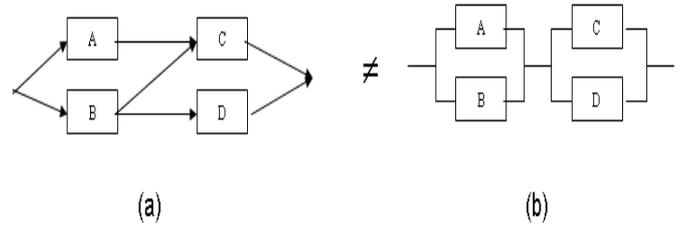


Fig. 3. Schéma de connexion et structure série-parallèle

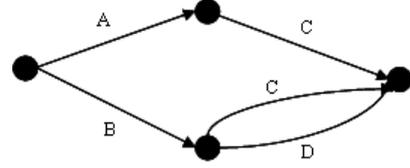


Fig. 4. Réseau de fiabilité correspondant à la figure 3-a

sons toutes les coupes ou tous les liens alors nous avons deux réseaux de fiabilité équivalents.

F. Pourquoi les réseaux de fiabilité ?

La raison principale de l'utilisation des réseaux de fiabilité est qu'ils permettent de modéliser tout type de structure complexe. Par exemple, la structure représentée dans la figure 3-a ne peut pas être représentée par la structure classique série parallèle de la figure 3-b (il manque une connexion entre A et D). Elle peut cependant être représentée par le réseau de fiabilité de la figure 4.

G. 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 l_i minimaux du réseau de fiabilité. La disponibilité instantanée est définie par l'équation :

$$A(t) = \sum_{i=1}^n P_{l_i}(t) \quad (7)$$

Où :

$P_{l_i}(t)$ 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 :

$$A(t) = P_{l_1}(t) + \bar{P}_{l_1}(t)P_{l_2}(t) + \dots + \bar{P}_{l_1}(t)\bar{P}_{l_2}(t)\dots\bar{P}_{l_{n-1}}(t)P_{l_n}(t) \quad (8)$$

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

$$A_{avg} = \frac{1}{T} \int_0^T A(t)dt \quad (9)$$

Où T est la période d'étude.

IV. ALGORITHMES GÉNÉTIQUES (AG)

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 (coût des composants).
- Les AG ont montré de très bonnes performances dans la résolution de problèmes d'allocation de fiabilité et de redondance pour lesquels il faut considérer de multiples critères d'optimisation [14], [15], [16], [8]. L'utilisation des AG pour l'allocation conjointe de disponibilité et de redondance paraît donc évidente.

A. Concepts de base

Un AG est un algorithme itératif de recherche d'optimum [17], [18]. 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. 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. Au fur et à mesure des générations, les chromosomes vont tendre vers un optimum de la fonction sélective.

B. Eléments de l'AG

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

B.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. Dans la littérature, nous trouvons deux types de codages, les codages en nombres réels et les codages binaires [18]. 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.

B.2 Population initiale

Une fois le codage choisi, une population initiale formée de solutions possibles du problème (chromosomes) doit être déterminée. La population initiale peut être générée aléatoirement, par duplication et évolution ou en s'appuyant sur une heuristique.

B.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.

B.4 Sélection

La sélection a pour objectif d'identifier les individus qui doivent se reproduire. Il existe plusieurs types de sélection [18]. 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.

B.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 [17], [18].

B.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. En général, nous choisissons une faible probabilité de mutation. Cette probabilité représente la fréquence à laquelle les gènes d'un chromosome sont mutés.

B.7 Choix des paramètres de l'AG

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, mais aussi des conditions initiales. Il n'y a pas de règle générale pour le choix de ces paramètres. Plusieurs auteurs [15], [16] 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 utiliser dans la suite de notre problème.

V. CAS D'APPLICATION

A. Application

Dans cette partie, nous proposons d'appliquer la méthodologie proposée à la conception optimale d'un SIS dont un SIL i est exigé. Nous utilisons une application concernant un réservoir sous pression définie dans le document technique ISA-TR84.00.02-2002 [19]. Notre objectif est de concevoir un SIS pour le réservoir dont le SIL i a été imposé au concepteur avec un coût total minimal. En conséquence, il faut choisir les composants de chaque sous système du

Composants du SIS	Sous systèmes					
	Capteurs		Unités de traitements		Actionneurs	
	c_1	p_1	c_2	p_2	c_3	p_3
Type 1	2100	0.039	1400	0.09	2500	0.1
Type 2	1500	0.07	2100	0.05	3500	0.06
Type 3	2000	0.03	1200	0.07	4100	0.04

TABLE II

COÛTS ET PROBABILITÉS DE DÉFAILLANCE DES COMPOSANTS DU SIS

SIS, ainsi que les connexions entre ces composants qui permettent d'obtenir le SIL exigé avec un coût de conception minimal. Notons que chaque composant ne peut être utilisé qu'une seule fois dans chaque partie du SIS.

Le problème de conception peut être ramené à un problème de minimisation du coût global du SIS sous une contrainte sur la disponibilité moyenne A_{avg} du SIS. La contrainte sur le SIL exigé est transformée en une contrainte sur la disponibilité moyenne du SIS selon le tableau I. Le coût global du SIS est la somme des coûts de ses composants. En outre, nous supposons qu'il y a 3 types de composants disponibles sur le marché pour chaque sous-système du SIS. Les probabilités de défaillance et les coûts des composants du SIS sont donnés dans le tableau II. Les coûts des composants représentent les prix moyens de ces composants sur le marché en Euros. Suite à de nombreux essais, les paramètres de l'AG que nous avons utilisés sont :

- Taille de la population : 200.
- Nombre de génération de la population : 300.
- Probabilité de croisement : 0.6.
- Probabilité de mutation : 0.05.

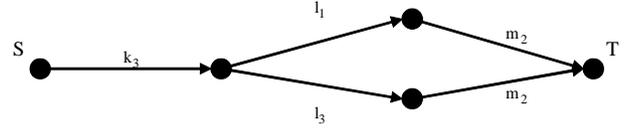
B. Résultats et analyse

Ayant défini toutes les données nécessaires (probabilités de défaillance et coûts des composants disponibles) pour traiter le problème d'optimisation, l'étape suivante est l'implémentation de la procédure de conception optimale pour différents SIL exigés dans l'exemple. En ce qui concerne l'optimisation, nous avons utilisé le logiciel MATLAB 7.1 et un processeur Intel(R) Pentium de 3.0 GHz. Les différents programmes d'optimisation ont été écrits sous MATLAB. Nous avons répété la procédure d'optimisation de l'AG 150 fois pour chaque SIL exigé.

B.1 Exigences SIL 1, SIL 2 et SIL 3

Les tableaux III, IV et V présentent les statistiques relatives aux résultats d'optimisation obtenus pour chaque SIL. Nous remarquons que pour tous les essais, les contraintes des SIL i ont été respectées puisque la disponibilité moyenne minimale obtenue est toujours supérieure au seuil exigé pour chaque SIL i . Nous avons choisi de donner les figures correspondant aux schémas de connexion et au réseaux de fiabilité des meilleures architectures obtenues pour le SIL 1 (cf. Figures 5 et 6) et le SIL 3 (cf. Figures 7 et 8) où k_i , l_i et m_i désignent respectivement le capteur type i , l'unité de traitement type i et l'élément final type i . Nous remarquons que nous obtenons pour un SIL 1 une structure

Statistiques	$C(x)$	$A_{avg}(x)$	SIL
Moyenne	8600	0.913037	1
Maximum	9400	0.927941	1
Minimum	8100	0.906056	1
Ecart type	661	0.0092	-

TABLE III
STATISTIQUES DU SIL1Fig. 5. Réseau de fiabilité (SIL1 : $A_{avg} = 0.906056$, $C = 8100$)

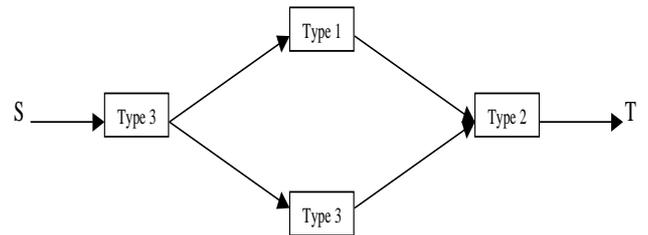
série parallèle et pour le SIL 3 une structure complexe.

C. Exigence SIL 4

Nous n'avons pas pu obtenir un SIL 4 puisque les données de fiabilité des composants utilisés ne le permettent pas (la valeur maximale de la disponibilité moyenne reste toujours inférieure à $A_{min} = 0.9999$ requis pour un SIL 4). C'est pourquoi, nous proposons l'utilisation de composants plus fiables que les précédents (cf. Tableau II) pour atteindre l'objectif SIL 4. Le tableau VI donne les paramètres de fiabilité des nouveaux composants utilisés. L'AG est exécuté 150 fois. La figure 9 présente le schéma de connexion de la meilleure architecture obtenue. Nous avons ainsi atteint notre objectif en utilisant des composants (cf. tableau VI) plus fiables que ceux utilisés précédemment (cf. Tableau II).

VI. CONCLUSION

Dans ce travail, nous avons proposé une méthodologie d'allocation conjointe de disponibilité et de redondance des composants des systèmes qui a été ensuite appliquée à la

Fig. 6. Schéma de connexion (SIL1 : $A_{avg} = 0.906056$, $C = 8100$)

Statistiques	$C(x)$	$A_{avg}(x)$	SIL
Moyenne	15000	0.992039	2
Maximum	16400	0.995124	2
Minimum	13400	0.990326	2
Ecart type	700	0.001176	-

TABLE IV
STATISTIQUES DU SIL2

Statistiques	$C(x)$	$A_{avg}(x)$	SIL
Moyenne	20400	0.99932	3
Maximum	20400	0.9994	3
Minimum	20400	0.9993	3
Ecart type	0	0.000121	-

TABLE V
STATISTIQUES DU SIL3

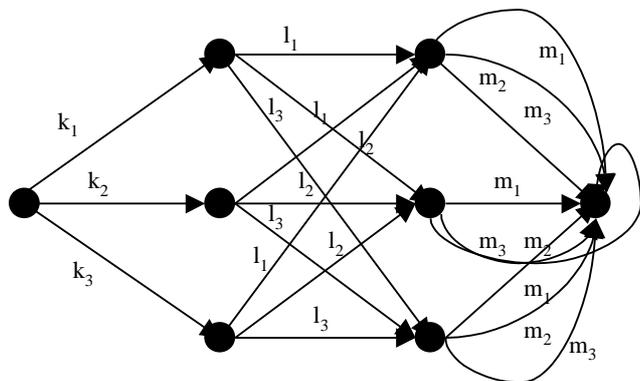


Fig. 7. Réseau de fiabilité (SIL3 : $A_{avg} = 0.9994$, $C = 20400$)

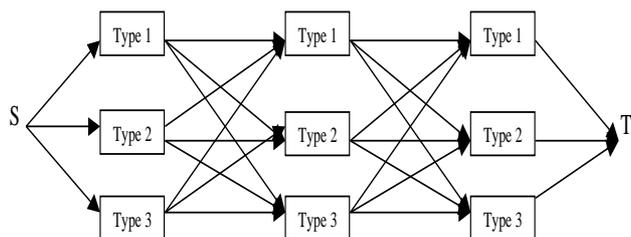


Fig. 8. Schéma de connexion (SIL3 : $A_{avg} = 0.9994$, $C = 20400$)

Composants du SIS	Sous systèmes					
	Capteurs		Unités de traitements		Actionneurs	
	c_1	p_1	c_2	p_2	c_3	p_3
Type 5	2100	0.019	1400	0.04	2500	0.02
Type 6	1500	0.03	2100	0.05	3500	0.03
Type 7	2000	0.022	1200	0.03	4100	0.04

TABLE VI
COÛTS ET PROBABILITÉS DE DÉFAILLANCE DES COMPOSANTS DU SIS
(TYPES 5, 6 ET 7)

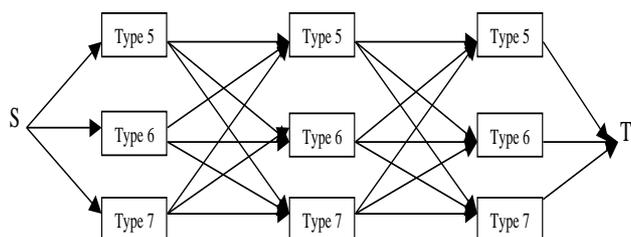


Fig. 9. Schéma de connexion (SIL4 : $A_{avg} = 0.9999003$, $C = 20400$)

conception 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 respectent les contraintes imposées pour chaque SIL exigé. L'intérêt des AG est le fait de présenter plusieurs architectures possibles est donc d'offrir plus de choix aux concepteurs selon d'autres critères non spécifiés dans le cahier des charges. Comme perspectives à ce travail, nous pouvons citer l'introduction de l'aspect du coût des connexions des composants ainsi que la prise en compte de la fiabilité des bus de communication dans les processus de conception optimale des systèmes.

RÉFÉRENCES

- [1] F. A. Tillman, C. L. Hwang, et W. Kuo. Optimization techniques for system reliability with redundancy : A review. *IEEE Transactions on Reliability*, 26 :148–155, 1978.
- [2] S. G. Tzafestas. Optimization of systems reliability : a survey of problems and techniques. *International Journal of Systems Science*, 11 :55–86, 1980.
- [3] B. S. Dhillon. *Human reliability*. Pergamon Press, 1986.
- [4] K. Misra. *On optimal reliability design : a review*. System Science, 1986.
- [5] W. Kuo. An annotated overview of system reliability optimization. *IEEE Transactions on Reliability*, 49 :176–187, 2000.
- [6] G. Levitin et A. Lisnianski. Joint redundancy and maintenance optimization for multi-state series-parallel systems. *Reliability Engineering and System Safety*, 64 :33–42, 1999.
- [7] H.P. Castro et K.L. Cavalca. Availability optimization with genetic algorithm. *International Journal of Quality and Reliability Management*, 20 :847–863, 2003.
- [8] C. Elegbede, C. Chengbin, K.H. Adjallah, et F. Yalaoui. Reliability allocation through cost minimization. *IEEE Transactions on Reliability*, 52 :106–111, 2003.
- [9] Iec 61508. functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems, 1998.
- [10] Iec 61511. functional safety : Safety instrumented systems for the process industry sector, 2000.
- [11] A. Kaufmann. *Introduction à la théorie des sous-ensembles flous-Éléments théoriques de base*, volume 1. Masson, 1977.
- [12] A. Kaufmann. *Introduction à la combinatoire en vue des applications*. Dunod, France, 1968.
- [13] A. Kaufmann. *Méthodes et modèles de la recherche opérationnelle*. Dunod, France, 1972.
- [14] M. Gen et R. Cheng. Optimal design of system reliability using interval programming and genetic algorithms. *Computers and Industrial Engineering*, 31 :237–240, 1996.
- [15] J.-E. Yang, M.-J. Hwang, T.-Y. Sung, et Y. Jin. Application of genetic algorithm for reliability allocation in nuclear power plants. *Reliability Engineering and System Safety*, 65 :229–238, 2000.
- [16] T. Yokota, M. Gen, et Y.-X. Li. Genetic algorithm for non-linear mixed integer programming problems and its applications. *Computers and Industrial Engineering*, 30 :905–917, 1996.
- [17] J. H. Holland. *Adaptation In Natural And Artificial Systems*. University of Michigan Press, 1975.
- [18] D. Goldberg. *Genetic algorithms*. Addison-Wesley, 1994.
- [19] Isa-tr84.00.02-2002. safety instrumented fonctions (sif), safety integrity level (sil), evaluation techniques, 2002.