Aide à la conception de Systèmes Instrumentés de Sécurité par les réseaux de fiabilité de Kaufmann

Frédérique Bicking, Christophe Simon, Mohamed Sallak, Jean-François Aubry

Aide à la conception de Systèmes Instrumentés de Sécurité par les réseaux de fiabilité de Kaufmann

Frédérique BICKING[1], Christophe SIMON[1], Mohamed SALLAK[2], Jean-François AUBRY[3]

[1]CRAN-Nancy Université-CNRS UMR 7039
ESSTIN, 2 Rue Jean Lamour, 54519 Vandœuvre-Les-Nancy, France

[2]HEUDIASYC-CNRS UMR 6599,
Université de Technologie de Compiègne, Centre de Recherches de Royallieu, BP 20529, 60205 COMPIEGNE Compiègne, France

[3]CRAN-Nancy Université-CNRS UMR 7039,
ENSEM, 2 Avenue de la Foret de Haye 54506 Vandoeuvre-Les-Nancy, France

Frederique.Bicking@esstin.uhp-nancy.fr, Christophe.Simon@cran.uhp-nancy.fr
mohamed.sallak@utc.fr, jean-francois.aubry@cran.uhp-nancy.fr

Résumé – Cet article propose l'étude de la conception de Systèmes Instrumentés de Sécurité (SIS) où une réduction des coûts est recherchée sous contrainte de disponibilité lors d'une sollicitation. L'article présente une approche offrant la possibilité de définir une structure complexe de SIS avec redondance diversifiée ce qui n'est pas le cas dans l'approche classique d'allocation de redondance. Pour ce faire, les réseaux de fiabilité de Kaufmann basés sur des multi-graphes sont utilisés. Quelques exemples de mises en oeuvre sont donnés sur un problème d'allocation de redondance diversifiée et sur la recherche de structures de connexion des composants intégrant la réduction des coûts de connexion pour obtenir des SIS qui satisfont aux niveaux d'intégrité et sécurité (SIL) cibles.

Abstract – This paper proposes the study of Safety Instrumented Systems (SIS) design where a reduction of design cost under availability constraints is searched. The paper also investigates the possibility to define a complex structure with diverse redundancies. For this purpose, a Kaufmann's reliability network approach based on multi-graphs is used. Some experiments are done first on a diverse redundancy allocation problem then on the structure definition and reduction of connection costs to obtain SIS that meets the required Safety Integrity Level (SIL) target.

1 Introduction

L'industrie de process devient techniquement de plus en plus complexe et le potentiel de danger s'accroit en conséquence si les flux de danger ne sont pas convenablement contrôlés. Ainsi, lorsque les installations industrielles présentent des risques potentiels pour les personnes, l'environnement ou les biens, diverses sécurités sont à mettre 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 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 [14] et l'IEC 61511 [15].

La mise en œuvre des prescriptions de ces deux normes est assez difficile et les méthodes proposées dans les annexes doivent être utilisées avec précaution [16]. Toutefois, un élément clairement établi dans le processus de conception d'un SIS est qu'il doit aboutir à la satisfaction d'un niveau d'Intégrité de Sécurité (SIL, Safety Integrity Level) alloué [29]. Le SIL exprime ainsi la réduction de risque que doit apporter un SIS au système qu'il surveille.

La contrainte d'une conception de SIS est donc de satisfaire au niveau de SIL requis tout en minimisant les coûts de conception, d'exploitation .... Il s'agit donc d'un problème d'optimisation où le coût doit être minimisé sous des contraintes de sureté de fonctionnement. La littérature offre peu de développement d'outils d'aide à la conception de SIS mais un grand nombre d'articles s'intéressent à la conception optimale de systèmes d'un point de vue des paramètres de sûreté de fonctionnement. Tillman *et al.* [32], Kuo *et al.* [22] et Tzafestas [34] ont publié des états de l'art sur les techniques d'optimisation de la fiabilité des systèmes. Dhillon [6] et Misra [27] ont proposé une liste de références sur l'allocation de la fiabilité. Yalaoui *et al.* [36] ont proposé une méthode d'allocation de fiabilité pour les systèmes séries-parallèles. Levitin *et al.* [24] 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.* [3] 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 de systèmes parallèle-séries basée sur les plans d'expérience afin de paramétrer l'algorithme génétique utilisé.

Toutes les méthodes proposées approchent le problème d'optimisation pour des systèmes dont la structure est de type parallèle-série. Dans cet article, nous présentons une approche générale de conception de SIS permettant de traiter aussi bien les systèmes parallèle-série que les systèmes complexes. Nous pro-

posons notamment la recherche de la structure de connexion des composants du SIS à concevoir en fonction des objectifs de niveau de d'intégrité de sécurité. Pour cela, nous utilisons les réseaux de fiabilité.

L'article est articulé autour de 4 sections. La deuxième section concerne les éléments essentiels de la norme, notamment sur les notions de niveaux de performance (SIL) et les contraintes architecturales de tolérances aux défaillances du matériel. La troisième section présente les notions utiles des réseaux de fiabilité de Kaufmann et leur exploitation pour le calcul de la disponibilité des SIS. La quatrième section expose la méthode d'optimisation et quelques résultats d'application sur des problèmes de complexité variable.

2 Eléments de normalisation

La norme IEC 61508 [14] 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, nucléaires, ferroviaires ...

La norme IEC 61508 [14] fixe le niveau d'intégrité de sécurité (SIL) qui doit être atteint par un SIS qui réalise la Fonction Instrumentée de Sécurité (SIF) dès lors qu'une réduction de risque est nécessaire. La norme fixe le SIL en fonction de la probabilité de défaillance moyenne sur demande (PFD_{avg}) pour les SIS faiblement sollicités (moins d'une sollicitation par an) ou en fonction de la probabilité de défaillance par heure (PFH) pour les SIS fortement sollicités ou agissant en mode continu (cf. tableau 1). L'allocation du SIL se fait par des méthodes qualitatives et semi quantitatives, alors que l'évaluation du PFD_{avg} des SIS qui doivent satisfaire au SIL exigé se fait par des méthodes quantitatives. Les méthodes usuelles de calcul du PFD_{avg} des SIS sont des méthodes probabilistes [14], [15], [10]. Elles sont issues des études traditionnelles de sûreté de fonctionnement où les données de fiabilité relatives aux composants (taux de défaillance, taux de réparation ...) peuvent être connues avec plus ou moins de précision et sont validées par le retour d'expérience.

SIL	Probabilité moyenne de défaillance à la sollicitation (PFD_{avg})	Fréquence des défaillances dangereuses par heure (PFH)
1	$[10^{-2}, 10^{-1}[$	$[10^{-6}, 10^{-5}[$
2	$[10^{-3}, 10^{-2}[$	$[10^{-7}, 10^{-6}[$
3	$[10^{-4}, 10^{-3}[$	$[10^{-8}, 10^{-7}[$
4	$[10^{-5}, 10^{-4}[$	$[10^{-9}, 10^{-8}[$

TAB. 1 – Niveaux d'intégrité de sécurité (SIL) : Sollicitation faible [14]

Pour mettre en œuvre un E/E/PE, il faut s'appuyer sur un ensemble de composants disponibles dans les catalogues de distributeurs. Un SIS peut être considéré comme un système d'automatique à 3 couches. L'architecture en couches est usuelle mais il s'agit d'une vision plus large que celle des systèmes série-parallèles. La première couche concerne la partie *capteur*. Elle est constituée d'un ensemble d'éléments d'entrée qui mesurent l'évolution des paramètres physico-chimiques caractéristiques de l'EUC (Entité Under Control). Cette évolution vers une situation dangereuse constitue la solliciation du SIS. La seconde couche concerne la partie *unité logique*. Sur la base de l'évolution des paramètres physico-chimiques, la ou les unités logiques élaborent une décision de mise en sécurité. La troisième couche concerne les *actionneurs* ou *éléments finaux* dont l'objectif est d'agir sur l'EUC directement ou indirectement pour neutraliser la dérive de l'EUC en la plaçant dans une situation de repli, un état sûr. Evidemment, la mise en sécurité influe directement sur la disponibilité de l'EUC avec d'éventuelles conséquences en terme de pertes de production. Il peut être envisagé de tenir compte de ces pertes essentiellement économiques dans la définition des SIS [13].

L'architecture solution est contrainte par la tolérance aux défaillances matérielles (cf. tableau 2) et la performance du SIS est obtenue grâce à de la redondance de composants, de canaux. Un canal représente une architecture série permettant d'assurer la fonction désirée. Ainsi, les architectures les plus connues (1oo1, 1oo2, 1oo3, 2oo3 ...) sont des combinaisons de canaux largement étudiés par Innal [17].

Proportion de défaillances en sécurité	Tolérance aux anomalies matérielles		
	0	1	2
$< 60\%$	Non Autorisé	SIL 1	SIL 2
$60\% \leq - < 90\%$	SIL 1	SIL 2	SIL 3
$90\% \leq - < 99\%$	SIL 2	SIL 3	SIL 4
$\geq 99\%$	SIL 3	SIL 4	SIL 4

TAB. 2 – Exemple de contraintes architecturales sur les E/EPE

Comme le précise Lundteigen [25], cette contrainte architecturale a été introduite car l'expérience a montré que la performance calculée du SIS était souvent supérieure à celle obtenue réellement. La contrainte a pour objectif de favoriser des architectures robustes aux défaillances matérielles et évite le choix d'architecture sur la seule base du PFD_{avg}. Ainsi, en faisant référence au tableau 2 par exemple, un objectif de SIL 2 contraint à une architecture avec une tolérance aux fautes matérielles de 2 si la proportion de défaillances en sécurité est inférieure à 60% et une tolérance de 1 si cette proportion est dans l'intervalle $[60\%, 90\%]$. Rappelons que cette proportion est liée au taux de couverture de diagnostic qu'il faut maîtriser quantitativement dans le contexte du E/E/PE développé sachant que l'IEC61508 tolère le retrait de certaines anomalies si leur occurence est jugée faible. Lundteigen [25] précise que la SFF (Safe Failure Fraction) n'a pas toujours une influence positive sur la sécurité car le SIS induit parfois des événements dangereux. Langeron [23] précise que les défaillances sûres évoluent parfois en défaillances dangereuses, ce qui ne crédibilise pas la valeur de la SFF. Lundteigen [25] argumente également sur le fait que le choix de la valeur de la SFF peut être conduit par des raisons de réduction de coûts, et que cette valeur n'est pas connue parfaitement pour tous les composants (notamment les actionneurs). De fait, la valeur du PFD peut être affectée par

des données de fiabilité peu crédibles.

3 Réseaux de fiabilité de Kaufman

Les réseaux de fiabilité sont une méthode très efficace pour calculer la disponibilité ou la fiabilité instantanée des systèmes [26, 20], c'est-à-dire la valeur $(1-PFD)$. Ils sont très utilisés dans l'étude des réseaux de communications ou de distribution d'énergie [28] car ils permettent de représenter sous forme de graphe la structure et les connexions d'un ensemble complexe en exprimant les relations entre ses éléments. Les graphes constituent un outil de modélisation pour de nombreux problèmes en se ramenant à l'étude des sommets et des arcs [5, 30]. Ainsi, ils offrent un moyen simple pour traiter du problème de structure des systèmes dans le cadre d'une optimisation de la fiabilité ou la disponibilité sans restriction structurelle comme dans les systèmes série-parallèles.

Comme l'a défini Kaufmann [19], un réseau de fiabilité est un multi-graphe $G = \langle N, A, U \rangle$ avec un ensemble N de n nœuds et un ensemble A d'arcs nommés a_{ij}. L'ensemble des arcs est défini comme $A \subseteq N \times N$. $U : A \mapsto e$ lie chaque arc a_{ij} à un composant e_i dans l'ensemble des composants $e = \{e_1, e_2, \ldots, e_r\}$ [19, 17]. D'après U, plus d'un arc peut être associé à un composant. Comme le but des arcs est de représenter les composants, les nœuds représentent les connexions, ce qui fixe la structure. Un réseau de fiabilité G est acyclique et contient un nœud source $S \in N$ sans arc entrant et un nœud terminaison $T \in N$ sans arc sortant. Dans un réseau de fiabilité, il est fait l'hypothèse d'états binaires des composants et du système. Kaufmann a ainsi montré qu'un réseau de fiabilité est une représentation graphique de la fonction de structure [19, p.79]. La fonction de structure d'un système est définie comme $\phi(x_1, x_2, \ldots, x_r) \mapsto \{0,1\}$ où les x_i représentent les états des composants.

Du réseau de fiabilité, nous pouvons énumérer l'ensemble des coupes minimales et l'ensemble des liens minimaux. Le multi-graphe représentant le réseau de fiabilité du système peut alors être réécrit comme un 1-graphe composé de l'ensemble des liens minimaux [19, p.78]. Le 1-graphe où chaque arc est associé à un composant du système est une nouvelle représentation de la fonction de structure. La fiabilité ou disponibilité du système peut alors être calculée par la méthode d'inclusion-exclusion [26] ou la somme des produits disjoints [35].

Ainsi, si nous sommes capable d'exprimer la fonction de structure par un réseau de fiabilité de type 1-graphe, alors nous sommes capable de concevoir une structure de systèmes répondant à des objectifs de performance sous contrainte de fiabilité ou de disponibilité, de tolérance aux défaillances matérielles ...

4 Aide à la conception : applications

L'étape de conception d'un SIS n'est pas particulièrement aisée à réaliser pour l'ingénieur fiabiliste. Il s'agit de choisir des composants du marché susceptible de répondre à la problématique de sécurité selon le type de process physico-chimique, le niveau de performance de réduction de risque, de contrainte architecturale liée à la norme, de coûts de conception et d'opération, éventuellement de poids et de volume. Il est possible de formaliser ce problème comme la recherche d'un réseau de fiabilité sous forme d'un 1-graphe assurant la minimisation des coûts sous différentes contraintes en puisant dans un lot de composants disponibles sur le marché. Ce type de problème est connu pour être NP-difficile et peut être résolu efficacement par des méta-heuristiques [31]. De nombreuses métaheuristiques voire des combinaisons de méthodes [37, 9, 21, 4] comme les algorithmes génétiques [2], les colonnies de fourmis, les essaims particulaires ... peuvent être utilisées. Nous avons choisi d'exploiter un algorithme génétique car nous en avons un certaine maîtrise, utile à la résolution d'un tel problème. Dans cet article, nous utilisons la méthode génétique précédemment élaborée par Bicking *et al.* [1] avec une définition particulière des chromosomes et des opérateurs appropriés de reproduction, combinaison et mutation. Toutes les contraintes relatives à la définition d'un SIS comme par exemple son SIL, sont prises en compte lors de la création des individus. Un individu est représenté par une chaîne de gènes représentant les paramètres du problème (les composants à connecter et leur connection d'une couche à l'autre). Une interprétation de cette chaîne est réalisée pour construire le réseau de fiabilité constituant une représentation d'une solution du problème. On détermine, pour ce réseau, les chemins de succès ou les coupes minimales et on vérifie la contrainte de tolérance aux anomalies matérielles. La disponibilité (ou fiabilité) du système est ensuite calculée et on vérifie la contrainte de SIL. Si cette contrainte est satisfaite, l'individu est intégré dans la population qui constitue un ensemble de solutions potentielles. Pour chaque individu, le coût est calculé et le critère recherché est un coût minimal. Le principe est d'effectuer itérativement des phases de sélection, de recombinaison et de mutation permettant de créer de nouveaux individus. L'adaptation d'un individu correspond à la fonction objectif du problème à optimiser. La stratégie globale est suffisamment élitiste pour éliminer les individus non adaptés (mauvaises solutions) et garder une certaine diversité pour que la population ne soit pas bloquée dans un minimum local.

Le principe des algorithmes génétiques étant largement connu [12, 11], nous ne le développerons pas plus dans cet article. En revanche, l'essentiel de l'effort de formalisation se concentre sur le codage dans l'algorithme pour résoudre le problème d'optimisation sous contraintes. Le premier problème que nous traitons est de considérer un système parallèle-série avec une allocation de redondance diversifiée. L'allocation de rendondance est un problème classique, qui a été largement étudié dans la littérature comme nous l'avons rappelé en introduction. En revanche, il n'a jamais été traité, à notre connaissance, par les réseaux de fiabilité de Kaufmann. L'allocation de redondance diversifiée est plus compliquée et notre approche s'avère efficace à le traiter. L'intérêt de rechercher ce type de redondance repose sur la réduction implicite du facteur de cause commune de défaillance [33].

Nous utilisons une application concernant un réservoir sous pression définie dans le document technique ISA-TR84.00.02-2002 [18]. Notre objectif est de concevoir un SIS pour le réservoir. Le SIL est imposé au concepteur et la demande est formulée avec un coût total minimal. En conséquence, il faut déterminer la structure du SIS, choisir les composants et leur type pour chaque sous système du SIS, ainsi que les connexions entre ces composants qui permettent d'obtenir le SIL exigé. La contrainte sur le SIL exigé est transformée en une contrainte sur la disponibilité moyenne du SIS selon le tableau 1. Le pro-

Type des composants du SIS	Sous-systèmes					
	Capteurs		Unités logiques		Eléments finaux	
	c_1	r_1	c_2	r_2	c_3	r_3
Type 1	21	0.961	14	0.91	25	0.90
Type 2	15	0.93	21	0.95	35	0.94
Type 3	20	0.97	12	0.93	41	0.96
Type 4	25	0.981	22	0.96	27	0.98
Type 5	45	0.99	26	0.99	28	0.97
Type 6	30	0.9775	22	0.97	31	0.99

TAB. 3 – Caractéristiques de coûts et de fiabilité des composants disponibles (types 1 à 6)

blème peut être ramené à un problème de minimisation du coût global du SIS sous une contrainte de disponibilité moyenne. La disponibilité moyenne 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 :

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

où $P_{l_i}(t)$ est la disponibilité instantanée du lien minimal i et n est le nombre de liens minimaux du réseau de fiabilité. Cette équation est calculée par disjonction des termes pour tenir compte de la répétition des évènements dans les liens minimaux. La disponibilité moyenne est obtenue par intégration sur le temps de fonctionnement ou le temps entre instants d'inspection ou de test.

Le coût global du SIS est la somme des coûts de ses composants intégrant les coûts d'achat et opérationnels (exploitation, maintenance, logistique ...). Les coûts opérationnels sont évalués a priori par l'ingénieur fiabiliste à partir du retour d'expérience. En outre, nous supposons qu'il y a 6 types de composants disponibles sur le marché pour chaque sous-système du SIS. Les fiabilités aux temps d'inspection et les coûts des composants du SIS sont donnés dans le tableau 3.

4.1 Allocation de redondance diversifiée pour un SIS à structure série-parallèle

Dans cette partie, nous définissons l'architecture du SIS comme un système parallèle-série dont chaque couche peut contenir de 1 à 6 composants. Les caractéristiques des composants disponibles sont définis dans le tableau 3. Le SIS est représenté comme sur la figure 1. Le problème est ici assez simple, il s'agit de choisir le ou les composants à placer dans chaque sous-système de manière à minimiser le coût global du système sous la contrainte de fiabilité exprimée par le niveau de SIL.

Le codage utilisé est une chaîne de 18 paramètres représentant les types des composants :

$$c_{11} \dots c_{1j} \dots c_{1c} c_{21} \dots c_{2j} \dots c_{2u} c_{31} \dots c_{3j} \dots c_{3f}$$

avec la convention suivante :

$$\begin{cases} 0, & \text{si il n'y a pas de composant} \\ 1, & \text{si le composant est de type 1 ;} \\ 2, & \text{si le composant est de type 2 ;} \\ 3, & \text{si le composant est de type 3 ;} \end{cases}$$

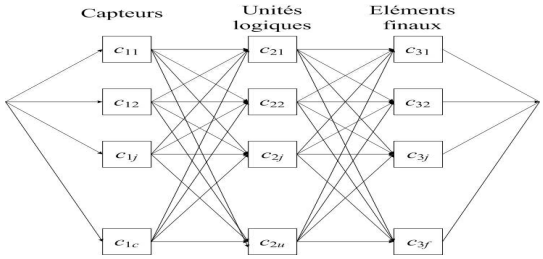

FIG. 1 – Schéma général d'un SIS à structure parallèle-série

Les résultats obtenus lors d'essais pour un SIS de SIL 4 exigé conduit au SIS présenté figure 2 et son réseau de fiabilité associé en 3. Le coût obtenu est de 184 unités pour une disponibilité moyenne de $A_{avg} = 0.99990499$. Cette structure de SIS présente une structure codée par [032030330330400404] composée de :

- 3 capteurs (types 2 et 3)
- 4 unités logiques (type 3)
- 3 éléments finaux (type 4)

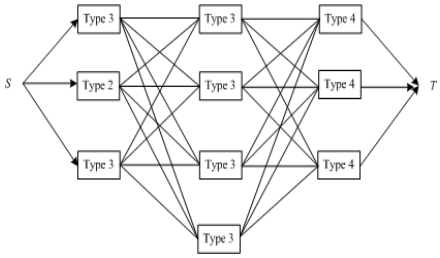

FIG. 2 – Schéma de connexion du SIS de SIL4 ($A_{avg} = 0.99990499$; $C = 184$)

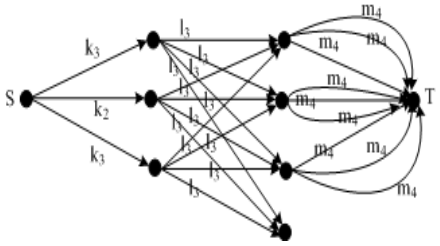

FIG. 3 – Réseau de fiabilité du SIS de SIL4 ($A_{avg} = 0.99990499$; $C = 184$)

Grâce à la méthode génétique, nous obtenons également d'autres configurations avec une fiabilité et un coût légèrement plus élevés. Un exemple de l'une de ces configurations est défini par le SIS codé par [002043333100400404 qui signifie composé de 3 capteurs (types 2,3 et 4), 4 unités logiques (types 1 et 3) et 3 éléments finaux de type 4. Le coût de ce SIS est $C = 191$ unités et sa disponibilité moyenne est $A_{avg} = 0.99992123$. Les autres configurations obtenues sont résumées dans le tableau 4.

4.2 Recherche de l'architecture du SIS

Le problème que nous traitons ici est la recherche simultanée des composants et de la structure de leurs connexions dans le respect de l'architecture des SIS pour satisfaire la performance de réduction de risque à coût minimal sous contrainte de redondance matérielle minimale. Le coût des connexions fait sens

SIL	code du SIS	coût	A_{avg}
4	[202022 330013 400041]	189	0.999905123
4	[020033 330103 604004]	190	0.999902132
4	[230003 031303 400056]	191	0.999900132
4	[002043 333100 400404]	191	0.999921232

TAB. 4 – Disponibilité moyenne et coût pour d'autres SIS de SIL 4

au regard du coût induit par les connectiques dans l'industrie de process, le coût opérationnel étant répercuté sur les composants.

Nous utilisons l'application concernant un réservoir sous pression définie dans le document technique ISA-TR84.00.02-2002 [18]. Comme dans le cas précédent, notre objectif est de concevoir un SIS pour le réservoir avec un SIL imposé. En conséquence, il faut déterminer la structure du SIS, choisir les composants et leur type pour chaque sous système du SIS, ainsi que les connexions entre ces composants qui permettent d'obtenir le SIL exigé avec un coût minimal. La contrainte sur le SIL exigé est transformée en une contrainte sur la disponibilité moyenne du SIS selon le tableau 1. Le problème peut être ramené à un problème de minimisation du coût global du SIS sous une contrainte de disponibilité moyenne du SIS calculée à partir de l'équation 1. Le coût global du SIS est la somme des coûts de ses composants intégrant les coûts d'achat et opérationnels et le coût des connexions entre les composants à raison d'une unité par connexion. Les caractéristiques des composants utilisables sont données dans le tableau 3.

Le codage utilisé est une chaine de 102 paramètres représentant les types des composants et leurs connexions d'un sous-système à un autre avec :

$c_{11} \dots c_{1j} \dots c_{1c} c_{21} \dots c_{2j} \dots c_{2u} c_{31} \dots c_{3j} \dots c_{3f}$
$l_1 \dots l_6 l_7 \dots l_{42} l_{43} \dots l_{78} l_{79} \dots l_{84}$

où les c_{ij} sont comme précédemment le type des composants (valeurs entières), $l_1 \dots l_6$ codent de manière binaire les liens entre la source S et les composants de la couche capteurs et $l_{79} \dots l_{84}$ codent ceux des composants de la couche finale au terminal T. Les valeurs $l_7 \dots l_{42} l_{43} \dots l_{78}$ codent l'existence des liens entre un composant d'une couche et les composants de la couche successive. Ainsi, si toutes les valeurs des l_i sont égales à un, la structure du SIS est entièrement connectée et on se ramène à un système série-parallèle.

Des recherches de structure ont été menées avec cette nouvelle définition du codage de la structure du SIS. La solution trouvée lors d'essais pour un SIS de SIL 3 exigé conduit au SIS présenté figure 4 et son réseau de fiabilité associé en 5. La structure de ce SIS n'est plus un système série-parallèle. Le coût est $C = 139 + 13 = 152$ unités et la disponibilité moyenne est $A_{avg} = 0.999033$. En réduisant le nombre de connexions, on aboutit à une disponibilité moyenne légèrement plus faible que dans le cas d'une allocation de fiabilité pour un système série-parallèle pour lequel on trouvait $A_{avg} = 0.999114$.

5 Conclusion

Dans ce travail, nous avons proposé une méthodologie d'aide à la conception de SIS qui permet l'allocation simultanée de fiabilité et de redondance diversifiée des composants tout en

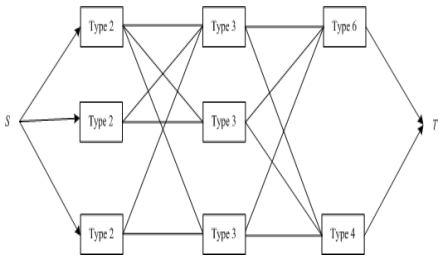

FIG. 4 – Schéma de connexion du SIS de SIL3 ($A_{avg} = 0.999033$; $C = 152$)

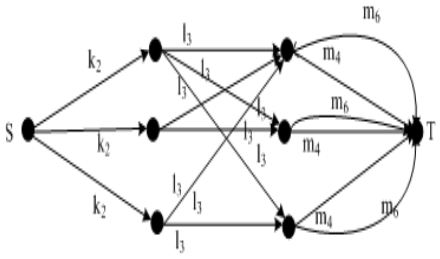

FIG. 5 – Réseau de fiabilité du SIS de SIL3 ($A_{avg} = 0.999033$; $C = 152$)

satisfaisant au niveau d'intégrité de sécurité (SIL) exigé par les normes de sécurité IEC 61508 et IEC 61511. Un premier intérêt de la méthodologie est d'aboutir à des structures où la redondance est non homogène ce qui réduit intuitivement l'importance des risques de défaillance de cause commune même si ce n'est pas l'objet direct de ce travail. Le second intérêt est d'obtenir des configurations qui ne sont pas de classiques architectures série-parallèle grâce à l'utilisation des réseaux de fiabilité pour la modélisation et le calcul de la fiabilité. Un troisième intérêt de la méthodologie est le fait de présenter plusieurs architectures possibles et donc d'offrir plus de choix aux concepteurs selon d'autres critères non spécifiés dans le cahier des charges. Enfin, nous pouvons préciser que la modélisation proposée reste ouverte à l'intégration d'éléments qui n'ont pas été modélisés ici comme le taux de défaillances de causes communes, le taux de couverture de diagnostic, l'intervalle de test, les coûts opératoires et de maintenance, la fiabilité des voteurs ...

Références

[1] F. Bicking, C. Fonteix, J-P. Corriou, and I. Marc, Global optimization by artificial life : a new technique using genetic population evolution. *RAIRO-Operations Research*, vol. 28(1), 23-36, 1994.

[2] H. Castro and K. Cavalca, Availability optimization with genetic algorithm, *International Journal of Quality and Reliability Management*, vol. 20, pp. 847–863, 2003.

[3] H. Castro and K. Cavalca, Maintenance resources optimization applied to a manufacturing system, *Reliability Engineering and System Safety*, vol. 91, pp. 413–420, 2006.

[4] D. Coit and A. Smith, Solving the redundancy allocation problem using a combined neural network/genetic algorithm approch, *IEEE Computer and Operation Research*, vol. 23, pp. 515–526, 1996.

[5] C. Colbourn, *The combinatorics of networks reliability*. Oxford University Press, 1996.

[6] B.S. Dhillon, *Design reliability : Fundamentals and applications*, CRC Press, 1999.

[7] F. Innal, Y. Dutuit, A. Rauzy, and J.-P. Signoret,New insight into pfdavg and pfh, Safety Users Group, July 2008. Available on http ://www.safetyusersgroup.com/documents/SR080001 /EN/SR080001.pdf

[8] C. Elegbede, C. Chengbin, K. Adjallah, and F. Yalaoui, Reliability allocation through cost minimization, *IEEE Transactions on Reliability*, vol. 52, pp. 106–111, 2003.

[9] M. Gen and R. Cheng, Optimal design of system reliability using interval programming and genetic algorithms, *Computers and Industrial Engineering*, vol. 31, pp. 237–240, 1996.

[10] W. M. Goble and H. Cheddie, *Safety Instrumented Systems verification : practical probabilistic calculations*. ISA, 2005.

[11] D. Goldberg, *Genetic algorithms*. Addisson-Wesley, 1994.

[12] J. H. Holland, *Adaptation In Natural And Artificial Systems*. University of Michigan Press, 1975.

[13] M.J.M Houtermans and J.L. Rouvroye, The influence of design parameters on the probability of failure on demand (PFD) performance of safety instrumented systems (SIS), 2005, Available on http ://www.safetyusersgroup.com/documents/PN050005/ EN/PN050005.pdf

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

[15] *IEC 61511. Functional safety : Safety Instrumented Systems for the process industry sector*, International Electrotechnical Commission Std., 2000.

[16] F. Innal, Y. Dutuit, and A. Rauzy, Some interrogations and remarks about CEI 61508, in *Proceedings of the Lambda Mu 2006 Conference, Lille, France*, 2006.

[17] F. Innal, Y. Dutuit, A. Rauzy, and J.-P. Signoret, New insight into PFD_{avg} and PFH, Safety Users Group, July 2008. Available on http ://www.safetyusersgroup.com/documents/SR080001 /EN/SR080001.pdf

[18] *ISA-TR84.00.02-2002. Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation techniques*, International Electrotechnical Commission Std., 2002.

[19] A. Kaufmann, D. Grouchko, R. Cruon, *Modèles mathématiques pour l'étude de la fiabilité des systèmes*, Masson, Ed., 1975.

[20] Y. Kim, A method for computing complex system reliability, *IEEE Transactions on Reliability*, vol. 21, pp. 215–219, 1972.

[21] W. Kuo, C. Hwang, and F. Tillman, A note on heuristic methods in optimal system reliability, *IEEE Transactions on Reliability*, vol. 27, pp. 320–324, 1978.

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

[23] Y. Langeron, A. Barros, A. Grall, and C. Bérenguer, Safe failure impact on safety instrumented systems, in *Proceeding of the Safety and Reliability Conference, ESREL'07*, T. Aven and J. Vinnem, Eds., vol. 1, Stavanger, Norway, 2007, pp. 641–648.

[24] G. Levitin and A. Lisnianski, Joint redundancy and maintenance optimization for multi-state series-parallel systems,*Reliability Engineering and System Safety*, vol. 64, pp. 33–42, 1999.

[25] M. Lundteigen and M. Rausand, Architectural constraints in iec61508 : Do they have intended effects ? *Reliability Engineering & System Safety*, vol. 94, pp. 520–525, 2009.

[26] K. Misra, An algorithm for the reliability of redundant networks, *IEEE Transactions on Reliability*, vol. 19, pp. 146–151, 1970.

[27] K. Misra, *On optimal reliability design : a review*. System Science, 1986.

[28] C.M. Rocco , J.A. Moreno, Network reliability assessment using celluler automata approach, *Reliability Engineering & System Safety*, vol. 78, pp. 289–295, 2002.

[29] M.Sallak, C. Simon, J.-FAubry, Optimal design of Safety Instrumented Systems : a graph reliability approach. *7ème Congrès International Pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita 2007, Tanger : Maroc (2007)*

[30] A. Satyanarayana and M. K. Chang, Network reliability and the factoring theorem, *Networks*, vol. 13, pp. 107–120, 1983.

[31] P. Siarry and Z. Michalewicz, Eds., *Advances in Metaheuristics for Hard Optimization*, ser. Natural Computing Series. Springer, 2008.

[32] F.A. Tillman, C-L. Hwang, and W. Kuo, *Optimization of system reliability*, Marcel Dekker, 1980.

[33] A. Torres-Echeverría, S. Martorell, and H. Thompson, Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy, *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 162 – 179, 2009.

[34] S. G. Tzafestas, Optimization of system reliability : A survey of problems and techniques. *International Journal System Science*, vol. 11, pp. 455-486, 2002.

[35] M. Veeraraghavan and K. Trivedi, An improved algorithm for symbolic reliability analysis, *IEEE Transactions on Reliability*, vol. 40, pp. 347–358, 1991.

[36] A. Yalaoui, E. Chatelet, and C. Chengbin, A new dynamic programming method for reliability and redundancy allocation in a parallel-series system, *IEEE Transactions on Reliability*, vol. 54, pp. 254–261, 2005.

[37] J.-E. Yang, M.-J. Hwang, T.-Y. Sung, and Y. Jin, Application of genetic algorithm for reliability allocation in nuclear power plants, *Reliability Engineering and System Safety*, vol. 65, pp. 229–238, 2000.