Aide à la conception de systèmes instrumentés de sécurité

Frédérique Bicking, Christophe Simon, Jean-François Aubry

AIDE À LA CONCEPTION DE SYSTÈMES INSTRUMENTÉS DE SÉCURITÉ
COMPUTER-AIDED DESIGN OF SAFETY INSTRUMENTED SYSTEMS

BICKING F. et SIMON C.
CRAN, Nancy Université, CNRS
ESSTIN, 2 Rue Jean Lamour
54519 Vandœuvre

AUBRY J.F.
CRAN, Nancy Université, CNRS
ENSEM, 2 Av. de la Foret de Haye, 54506
54506 Vandœuvre

Résumé

Cet article propose une méthodologie de conception des Systèmes Instrumentés de Sécurité (SIS) à un coût minimal 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 réseaux de fiabilité. La méthode d'optimisation choisie est les algorithmes génétiques permettant la recherche des composants à connecter ainsi que d'une structure de connexion de ces composants. La méthode est appliquée à la conception de SIS de SIL2 et SIL3, sur la base de structures de type parallèle série puis de structure plus atypique grâce à un codage approprié.

Summary

This article deals with a design methodology of Safety Instrumented System with a minimal cost and a safety integrated level constraint defined by standards IEC 61508 and IEC 61511. The proposed study involved in the context of availability and redundancy allocation of SIS. It is based on reliability graphs to model SIS. The optimisation method chosen is the genetic algorithms that allow searching the components to connect and the connection structure. The proposed methodology is applied to design SIS of SIL2 and SIL 3, based on usual parallel-series structures then on non-trivial structures thank to an appropriate coding.

1. Introduction

L'industrie de process devient techniquement de plus en plus complexe et le potentiel de danger s'accroît 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 (SIS) 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 [1] et l'IEC 61511 [2]. La mise en œuvre des prescriptions de ces deux normes n'est pas forcément triviale et les méthodes proposées dans les annexes doivent être utilisées avec précaution [3]. 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 [4]. 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 le coût de conception, le coût d'exploitation ... Il s'agit donc d'un problème d'optimisation où le coût doit être minimisé sous des contraintes de sûreté de fonctionnement. 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 conséquence, il est primordial de trouver une stratégie d'allocation de paramètres de sûreté de fonctionnement des composants du SIS qui permet d'établir le meilleur compromis entre le SIL requis et le coût de conception du SIS.

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. [5,6] et Tzafestas [7] ont publié des états de l'art sur les techniques d'optimisation de la fiabilité des systèmes. Dhillon [8] et Misra [9] ont proposé une liste de références sur l'allocation de la fiabilité. Yalaoui et al. [10] ont proposé une méthode d'allocation de fiabilité pour les systèmes séries-parallèles. Levitin et al. [11] 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. [12] ont également présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de maintenance. Elegbede et al. [13] ont développé une méthodologie d'optimisation de la disponibilité basée sur les plans d'expérience afin de paramétrer l'algorithme génétique utilisé. Tous ces travaux traitent soit des problèmes d'allocation de fiabilité soit d'allocation de redondance. Or, la conception de SIS englobe ces deux problématiques. Aussi, il est nécessaire de trouver une technique qui autorise ou traite de l'allocation de fiabilité (ou disponibilité) et de redondance simultanément (conjointement). En outre, les méthodes classiquement utilisées en optimisation de fiabilité s'appuient sur l'hypothèse de systèmes à structures de type paralèlle-série et privilégient la redondance de composant identique en négligeant le facteur de cause commune à laquelle la redondance non homogène de composants apporte une réduction.

Dans cet article, nous proposons une méthodologie d'optimisation pour la conception de SIS permettant d'assurer la réduction du coût de conception sous contrainte de disponibilité à partir de composants types, sans privilégier la redondance de composants identiques, ni de structure nécessairement parallèle série. Les difficultés majeures de ce problème résident dans l'élaboration du codage permettant la définition d'une structure de connexion entre composants, le choix des composants parmi ceux disponibles et le calcul de la disponibilité du système en fonction de sa structure. A cette fin, nous utilisons un algorithme évolutionnaire pour l'optimisation car il s'agit d'un problème NP-difficile, et nous le couplons aux réseaux de fiabilité pour calculer la disponibilité du SIS à partir des structures de connexion que peut proposer l'algorithme évolutionnaire. La section 2 de cet article concerne les SIS et les réseaux de fiabilité, la section 3 présente succinctement le problème d'optimisation. Enfin, la dernière section s'intéresse à des cas concrets.

2. SIS et réseaux de fiabilité

Système Instrumenté de Sécurité

Un Système Instrumenté de Sécurité est composé de 3 couches : capteurs, unités logiques et actionneurs (cf. Figure 1). Chaque couche comprend au maximum *m* composants pouvant être de types différents (redondance non homogène)

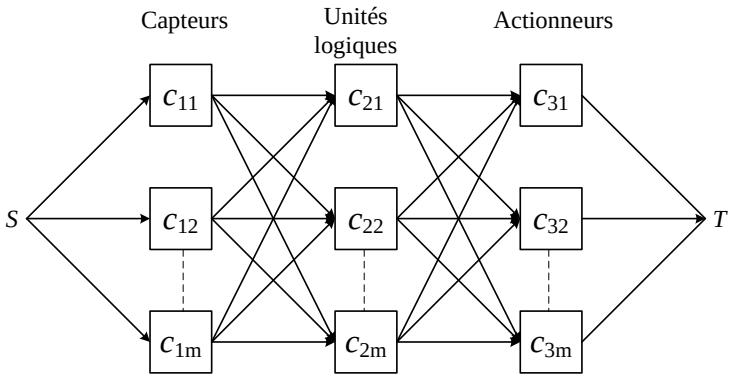


Figure 1 : Structure générale d'un SIS

La performance d'une fonction instrumentée de sécurité associée à un SIS se mesure en terme de probabilité de défaillance sur demande (PFDavg) sur une période donnée que l'on qualifie par un niveau de SIL. Les normes ANSI/ISA S84.01-1996 [14] et IEC 61508 [1] définissent les niveaux de SIL en fonction du mode de sollicitation des SIS comme le précise la table 1.

Sollicitation	Faible	Elevée
SIL	*PFDavg*	Défaillance/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	$[10^{-5};10^{-4}[$	$[10^{-9};10^{-8}[$

Table 1: Définition du SIL selon le mode de sollicitation.

Dans de nombreux articles sur l'allocation de fiabilité, la méthode d'optimisation se base sur un bloc diagramme de fiabilité. Or, les blocs diagrammes de fiabilité privilégient la représentation de systèmes parallèle-série ou série-parallèle. En conséquence, le calcul de la fiabilité dans ce cadre est aisé, mais aucune structure non triviale ne peut émerger. Ainsi, pour travailler sur la définition de la structure du SIS, il est nécessaire d'utiliser un autre mode de représentation. Les réseaux de fiabilité proposés par Kaufmann et al. [15] sont une alternative séduisante.

Réseau de fiabilité

Les réseaux de fiabilité sont des outils de représentation et de calcul efficaces pour la détermination de la fiabilité des systèmes. Ils permettent une modélisation de structures complexes aussi bien que de structures plus traditionnelles [16,15]. Un graphe de fiabilité G est un ensemble de nœuds (V), représentant les points de connexion du système, et de liens (E), représentant les composants du système à modéliser. Les nœuds sont liés entre eux par les liens et l'ensemble des liaisons peut être matérialisé par une matrice d'incidence. Le graphe contient un nœud source S et un nœud terminaison T. Il existe un ou plusieurs chemins entre les nœuds S et T et on peut déterminer pour le graphe l'ensemble des chemins liant S et T ainsi que l'ensemble des coupes. On peut également déterminer l'ensemble des chemins ou des coupes minimaux. Les liens représentant les composants du système, on en déduit les coupes minimales ou les chemins minimaux et par la somme de produits disjoints (SDP) [17,18] la fiabilité du système est obtenue. 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 2-a ne peut pas être représentée par la structure classique série parallèle de la figure 2-b (il manque une connexion entre A et D). Elle peut cependant être représentée par le réseau de fiabilité de la figure 3.

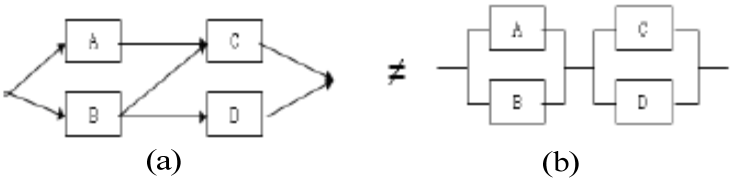


Figure 2 : Structure de connexion (a) et structure série-parallèle (b)

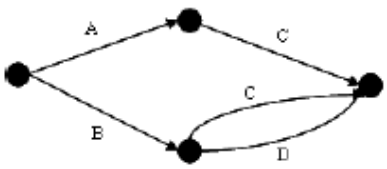


Figure 3 : Réseau de fiabilité correspondant à la figure 2-a

On peut remarquer que les SIS sont des systèmes à trois couches aussi, le graphe de fiabilité présente une structure simplifiée où les chemins de succès sont nécessairement minimaux. Le calcul de la fiabilité s'en trouve donc simplifié.

3. Recherche de structure

La conception du SIS consiste à déterminer les composants à mettre en œuvre et, comment connecter ces composants tout en vérifiant les contraintes de niveau de SIL en ayant un coût de conception minimal. Il ne s'agit donc pas d'un problème classique d'allocation de fiabilité et de redondance comme cela est généralement traité dans la littérature. En outre, la minimisation du coût sous contrainte de disponibilité est un problème NP-difficile trouvant solution grâce à des méta-heuristiques. Nous avons choisi les algorithmes évolutionnaires car ils sont faciles à mettre en œuvre, ne font pas d'hypothèse sur la fonction à optimiser, et combinent judicieusement exploration et exploitation [19].

En outre, ils ont montré de très bonnes performances dans la résolution de problèmes d'allocation de fiabilité et de redondance sur lesquels peu d'informations sont disponibles ou pour lesquels il faut considérer de multiples critères d'optimisation (Kuo et al., 2000). L'algorithme utilisé est l'algorithme évolutionnaire proposé par Bicking et al. [20] reposant sur une méthode génétique hybride. Cet algorithme a montré de bonne performance sur des problèmes NP-difficiles.

Le problème d'optimisation traité ici, nécessite également quelques hypothèses raisonnables:

- Seule la défaillance des composants est considérée.
- La liste des composants utilisables est préalablement connue i.e. les caractéristiques des composants (coût, taux de défaillances) sont connues et fixes.
- Le coût du système est la somme des coûts de ses composants

La fonction à minimiser est définie comme la fonction objectif et représente le coût du SIS, qui s'écrit :

$$C_S = \sum_j \sum_i C_{ij} \qquad [1]$$

Où C_s est le coût de conception du système, C_{ij} le coût du i^{ème} composant dans la couche j. A des fins de généralisation, on peut aisément considérer les coûts opératoires et de maintenance associés à chaque composant dés lors que nous pouvons les chiffrer.

Le coût est à minimiser sous la contrainte de fiabilité définie par :

$$R_{\min} \le R_S \le R_{\max} \qquad [2]$$

Où R_S est la fiabilité du SIS et $R_{\min} = 1 - \min(PFD_{avg})$, $R_{\max} = 1 - \max(PFD_{avg})$ ses bornes qui sont définies à partir du niveau de SIL cible (cf. table 1).

L'algorithme évolutionnaire utilisé ne travaille pas directement avec les solutions possibles du problème mais avec une représentation codée de celles-ci. Ce codage utilisé par l'algorithme représente la structure du SIS. La structure générale d'un SIS (fig 1), peut-être définie comme un système à 3 couches (n=3) et *m* composants au maximum par couche. Aussi le codage de la structure du SIS est défini par un vecteur $x = [a_1\, a_2 \ldots a_m]$. De plus, comme chaque composant c_{ij} (i=1, …, n ; j=1, …, m) peut avoir des caractéristiques de fiabilité et de coût différentes en fonction de leur type connu a priori dans une liste de composants utilisables (ou catalogue), on définit les valeurs des a_i par les types de composants utilisés. Ainsi, ce vecteur représente les $n \times m$ composants et leur type avec la convention suivante :

$$\begin{Bmatrix} 0 & \text{, si le composant n'est pas connecté} \\ 1 & \text{, si le composant est du type 1} \\ 2 & \text{, si le composant est du type 2} \\ k & \text{, si le composant est du type k} \end{Bmatrix}$$

L'hypothèse de départ est que si le composant d'une couche *i* est présent, il est considéré comme connecté aux autres composants des couches *i*-1 et *i*+1 selon la figure 1. Si le composant est présent, donc connecté, le codage (vecteur *x*) indique son type. A partir de ce vecteur de codage définissant la structure du SIS, on construit le réseau de fiabilité correspondant afin d'évaluer sa disponibilité. 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 : $A(t) = \sum_{i=1}^{l} P_{l_i}(t)$ où $P_{l_i}(t)$ est la disponibilité instantanée du lien minimal *i* et *l* 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 : $A(t) = P_{l_1}(t) + \overline{P}_{l_1}(t) P_{l_2}(t) + \ldots + \overline{P}_{l_1}(t)\overline{P}_{l_2}(t) \ldots \overline{P}_{l_{l-1}}(t) P_{l_l}(t)$

Le calcul de disponibilité moyenne A_{avg} du SIS, où T est la période d'étude, est donné par :

$$A_{avg} = \frac{1}{T}\int_0^T A(t)dt \qquad [3]$$

La fiabilité du système instrumenté de sécurité R_S est considérée comme égale à la disponibilité moyenne A_{avg} du SIS car nous nous plaçons dans le cas de systèmes non réparables.

Le grand intérêt des graphes de fiabilité est qu'ils permettent le calcul de la fiabilité de systèmes quelque soit leur structure. Toutefois, quelques hypothèses classiques sont à formuler:

- La fonction de structure du système est cohérente.
- Les composants du système sont s-indépendants.
- Le système et ses composants n'ont que deux états.

L'algorithme évolutionnaire utilisé est une variante des classiques algorithmes génétiques. Basé sur les principes naturels de sélection et recombinaison des individus, cet outil d'optimisation manipule une population d'individus (vecteur des variables de décision) qui sont évalués à travers leur adaptation (fitness ou fonction objectif à optimiser). Des opérateurs génétiques tels que la mutation et la recombinaison permettent l'évolution des populations en sélectionnant et recombinant ceux dont l'adaptation est la meilleure. Ainsi, de génération en génération, seuls les meilleurs individus sont conservés. A terme, la méthode utilisée présente une population constituée des solutions optimales ou quasi optimales. La simplicité de mise en œuvre de cet outil nous a permis de l'utiliser pour l'optimisation structurelle de SIS. Un exemple de détermination de SIS à structure en couches, définie sous contraintes de cout et de choix des composants à caractéristiques variées, illustre l'utilisation de l'approche.

4. Etude de cas

Considérons le problème d'un SIS à concevoir formé de 3 couches avec au plus 3 composants par couche (cf. figure 4). La liste des composants disponibles est fournie à la table 2.

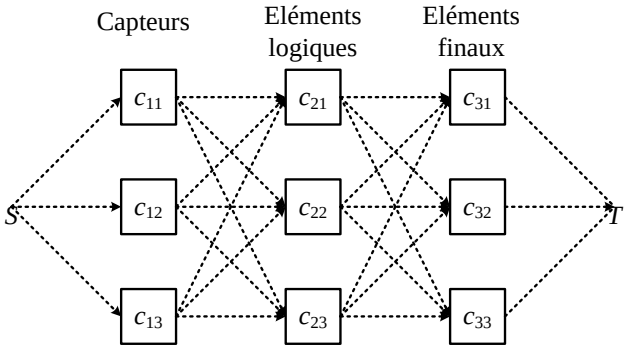


Figure 4 : Structure générale d'un SIS à n=3 couches et au maximum m=3 composants par couche

Composants du SIS	Sous-systèmes					
	Capteurs		Eléments logiques		Eléments finaux	
	c1 (unités)	r	c2 (unités)	r	c3 (unités)	r
Type 1	21	0,961	14	0,91	25	0,94
Type 2	15	0,93	21	0,95	35	0,96
Type 3	20	0,97	12	0,93	41	0,921

Table 2: Caractéristiques de coût et de fiabilité des composants disponibles.

Nous appliquons la méthode précédemment décrite à ce type de SIS et montrons les résultats obtenus pour différents niveaux de SIL. Le codage de la structure consiste en la définition d'un vecteur représentant le type de composant présent à chaque place disponible dans le SIS. Si on définit 3 places par étage, le vecteur est de taille 9. La population initiale est générée aléatoirement et elle évolue de génération en génération par l'application d'opérateurs d'évolution (combinaison et mutation). Après convergence, l'individu le mieux adapté est la meilleure solution, optimale ou quasi optimale, et représente la structure du SIS répondant aux critères de cout et de SIL.

A titre d'exemple, la méthode génétique a abouti à la solution présentée figure 5, à partir des caractéristiques des composants données table 1. Le type des composants est également indiqué par la notation $c_{ij}(k)$ ce qui signifie que le j^{ème} composant de la i^{ème} couche est du type (k). Pour la structure présentée figure 5, le vecteur *x*= [003033100] indique que seuls les composants c_{13}, c_{22}, c_{23} et c_{31} sont présents et connectés entre eux et que leur type sont respectivement un capteur de type 3, deux unités logiques de type 3 et un actionneur de type 1. La contrainte de niveau d'intégrité de sécurité est ici définie de niveau 1 (SIL 1) : $0.90 \le R_S \le 0.99$. Le coût calculé de ce système vaut $C_S = 69$ unités et sa fiabilité est $R_S = 0.9073$.

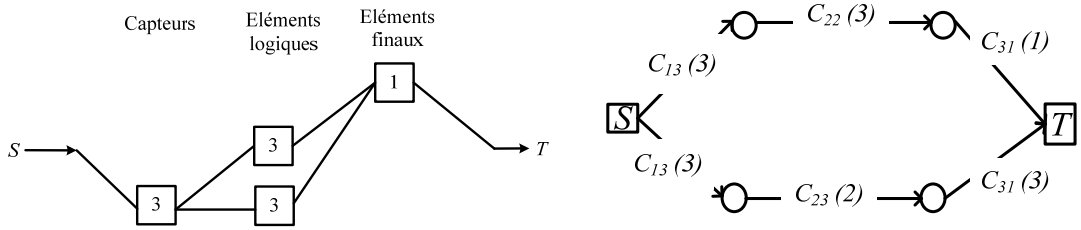
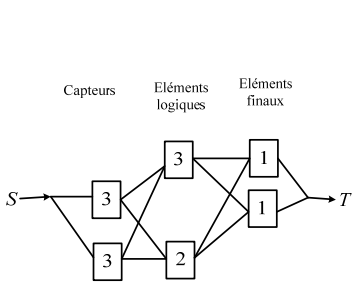
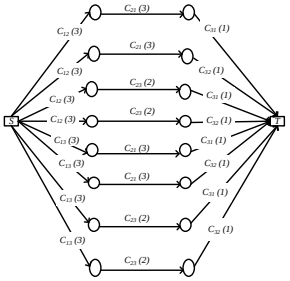


Figure 5**:** Structure [003033100] du SIS déterminée pour un SIL 1 et son réseau de fiabilité

Pour un SIL 2, la contrainte s'écrit : $0.99 \le R_S \le 0.999$. La méthode génétique donne la structure du SIS présentée sur la figure 6a. La figure 6b montre le réseau de fiabilité correspondant. Le coût de ce système de SIL 2 vaut $C_S = 123$ unités et sa fiabilité est $R_S = 0.99049$.



a) Structure du SIS de SIL 2



b) réseau de fiabilité correspondant

Figure 6 : Structure [033302110] du SIS déterminée pour un SIL 2 et son graphe de fiabilité

Les résultats montrent que la contrainte d'un SIL plus élevé impose la présence de composants supplémentaires ce qui reste logique puisque la fiabilité doit être accrue. Cependant, les structures trouvées sont de typologie classique (série-parallèle) du fait du codage adopté. C'est pourquoi nous avons modifié le codage utilisé afin d'autoriser l'apparition et la détermination de structures moins classiques. Nous proposons de modifier le vecteur de codage en y intégrant la connexion entre les composants. Ce vecteur est alors défini par : $x = [a_1\, a_2 \ldots a_m\, l_1\, l_2\, l_3\, l_4 .. l_{21} l_{22}\, l_{23}\, l_{24}]$ où les $a_1\, a_2 \ldots a_m$ sont comme précédemment le type des composants (valeurs entières), $l_1\, l_2\, l_3$ codent de manière binaire les liens entre la source S et les composants de la première couche c_{1j} (j=1, …, 3) et $l_{22}\, l_{23}\, l_{24}$ codent ceux des composants de la troisième couche c_{3j} (j=1, …, 3) au terminal T. Les valeurs $l_4 .. l_{21}$ 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 comme celle de la figure 6a.

Des recherches de structure ont été menées avec cette nouvelle définition du codage de la structure du SIS. Afin de voir émerger des topologies atypiques, nous avons testé notre méthode avec un choix plus important des composants (6 types table 3).

Composants du SIS	Sous-systèmes					
	Capteurs		Eléments logiques		Eléments finaux	
	c1 (unités)	r	c2 (unités)	r	c3 (unités)	r
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

Table 3: Caractéristiques de coût et de fiabilité des composants disponibles

Les résultats obtenus pour un SIL 2 puis un SIL 3 sont présentés ci-dessous. Pour des raisons de lisibilité, nous ne présentons que les neuf premiers éléments du vecteur de codage, les autres se déduisant par la représentation graphique du SIS où apparaissent les liens déterminés comme existants.

Le premier test concerne un SIL 2. La topologie trouvée n'est plus classiquement série-parallèle comme le montre la figure 7.

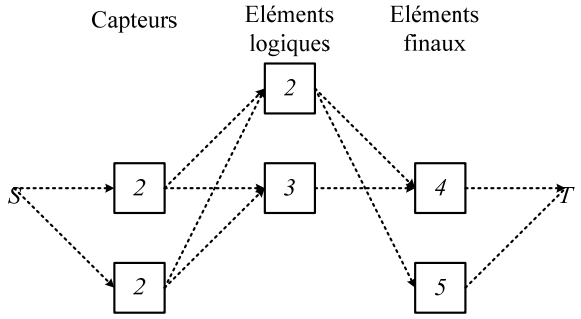


Figure 7 : Structure [022 230 045] du SIS déterminée pour un SIL 2 avec R=0.99012 et un cout de C=118

Le second test concerne un SIL 3. La meilleure topologie trouvée par la méthode génétique proposée est présentée sur la figure 8. Cette structure n'est pas purement série-parallèle, ce qui nous intéresse particulièrement. De plus, cette structure ne peut pas être représentée par un diagramme de fiabilité d'où l'intérêt d'utiliser les réseaux de fiabilité. Le coût de ce système est $C_s = 144$ et sa fiabilité vaut $R_S = 0{,}99901$.

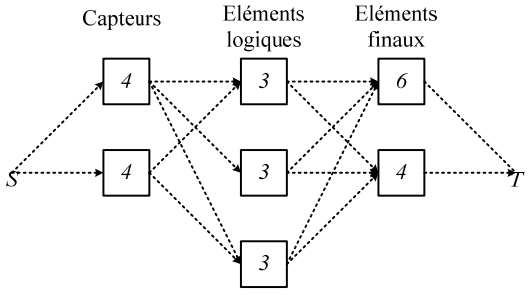


Figure 8 : Structure [440 333 640] du SIS déterminée pour un SIL 3 avec $R_S = 0{,}99901$ et un coût de $C_s = 144$

Ces deux exemples montrent l'intérêt de la méthode permettant d'obtenir une structure correspondant à un objectif de coût minimum et respectant la contrainte de niveau de sécurité intégrité définie.

Un autre intérêt de cette méthode est de disposer d'autres solutions quasi-optimales en terme de coût mais à fiabilité également plus élevée. C'est le cas du SIS de SIL 2 présenté à la figure 7 pour lequel une autre configuration codée par [022 630 045] a été déterminée avec une fiabilité $R_S = 0{,}9924$ et un coût de $C_S = 119$ avec mêmes liens. La différence entre ces deux solutions ne porte que sur la sélection des composants. De même, pour un SIS de SIL 3, on peut obtenir une variante de celui de la figure 8 par la sélection des composants et des liens ou connexions entre les composants. On obtient un système dont le cout est plus élevé (148 unités au lieu de 144) mais dont la fiabilité est également plus élevée (0,9992 au lieu de 0,99901) (figure 9).

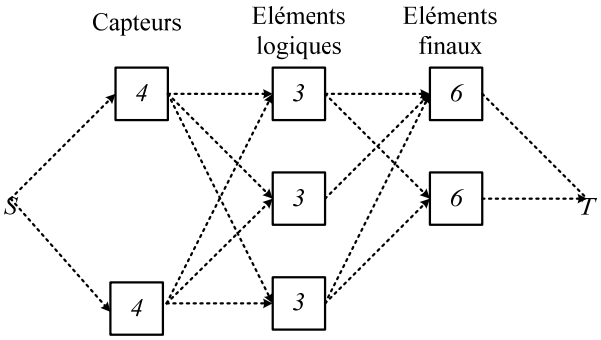


Figure 9 : Structure [404 333 660] du SIS déterminée pour un SIL 3 avec $R_S = 0{,}99992$ et un cout de $C_S = 148$

Ce dernier exemple montre que les multiples solutions déterminées par la méthode donnent de la flexibilité au processus de décision. En effet, dans le contexte économique des SIS pour lesquels les composants sont onéreux, notre démarche apparaît comme une voie intéressante permettant ainsi aux concepteurs de faire leurs propres choix parmi plusieurs structures disponibles impliquant des composants de caractéristiques différentes.

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 des composants tout en 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 …

6. Références

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

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

[3] Innal, F.; Dutuit, Y. & Rauzy, A. Quelques interrogations et commentaires relatifs à la norme IEC 61508 Proceedings of the Lambda Mu 2006 Conference, Lille, France, 2006

[4] Sallak M., Evaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : Application aux Systèmes Instrumentés de Sécurité. Thèse de doctorat, Institut National Polytechnique de lorraine, Nancy, France, 2007.

[5] F.A. Tillman, C-L. Hwang, and W. Kuo, Optimization techniques for system reliability with redundancy - a review, IEEE Transactions on Reliability, vol. 26, pp. 148-155, 1977.

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

[7] S. G. Tzafestas. Optimization of systems reliability : a survey of problems and techniques. International Journal of Systems Science, 11 :55–86, 1980.

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

[9] K. Misra, On optimal reliability design: a review, System Science, vol. 12, pp. 5-30, 1986.

[10] A. Yalaoui, E. Chatelet and C. Chu, 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.

[11] 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.

[12] H.P. Castro and K.L. Cavalca, Availability optimization with genetic algorithm, International Journal of Quality and Reliability Management, vol. 20, pp. 847-863, 2003.

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

[14] ANSI/ISA-S84.01-1996, Application of Safety Instrumented Systems for the process control industry, Instrumentation Society of America (ISA), 1996.

[15] Kaufmann, A.; Grouchko, D. & Cruon, R. Modèles mathématiques pour l'étude de la fiabilité des systèmes Masson et Cie, France, 1975

[16] R.A. Sahner, K.S. Trivedi and A. Puliafito, ACM Performance and Reliability Analysis of Computer Systems, Kluwer Academic Publishers,1996.

[17] S. Rai, M. Veeraraghavan, and K.S.Trivedi, A suvey of efficient reliability computation using disjoint products approach, IEEE Networks, vol. 25, pp. 147-163, 1995.

[18] M. Veeraraghavan and K.S. Trivedi, An improved algorithm for symbolic reliability analysis, IEEE Transaction on Reliability, vol. 40, pp. 347-358, 1991.

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

[20] 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.