Aide à la Conception de Systèmes Instrumentés de Sécurité par les Réseaux de Fiabilité

Frédérique Bicking[*,**] **& Christophe Simon** [**,***]

** IUT Nancy Brabois – Université Henri Poincaré*
Département QLIO, 2 rue du Colonnel Clarenthal, 54300 Lunéville
*** CRAN, Nancy-Université-CNRS, UMR 7039, 2 Rue Jean Lamour, Vandoeuvre les Nancy*
**** IUT d'Epinal Hubert CURIEN, Université de Nancy 2*
Département QLIO, 7 Rue des Fusillés de la Résistance, 88010 Epinal

frederique.bicking@iutnb.uhp-nancy.fr ; christophe.simon@univ-nancy2.fr

Sections de rattachement : 61
Secteur : Secondaire

RÉSUMÉ. Cet article propose une méthodologie de détermination de structure, d'allocation conjointe de disponibilité et de redondance des composants de systèmes instrumentés de sécurité (SIS). La méthodologie est basée sur l'utilisation des réseaux de fiabilité et des algorithmes génétiques pour la recherche de configurations optimales. En guise d'illustration, la méthodologie est appliquée à la conception d'un Système Instrumenté de Sécurité défini dans le document ISATR84.00.02-2002 relatif à la norme IEC 61508. Un premier exemple concerne la conception d'un SIS devant satisfaire à un niveau de SIL fixé sous contrainte de coût minimal à partir d'un choix de composants entièrement connectés. Le second exemple intègre des coûts de connexion impliquant la détermination d'une structure non parallèle série.

MOTS-CLÉS : Sécurité, Aide à la Conception, Réseaux de fiabilité, Algorithmes génétiques

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 (IEC, 1998) et l'IEC 61511 (IEC, 2004).

La mise en œuvre des prescriptions de ces deux normes est assez difficile et les méthodes proposées dans leurs annexes doivent être utilisées avec précaution (Innal et al., 2006). 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) alloué (Sallak, 2008). 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, d'exploitation ... Il s'agit donc d'un problème d'optimisation où le coût doit être minimisé sous des contraintes de performance 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. (1977), Kuo et al. (2001) et Tzafestas (1980) ont publié des états de l'art sur les techniques d'optimisation de la fiabilité des systèmes. Dhillon (1999) et Misra (1986) ont proposé une liste de références sur l'allocation de la fiabilité. Yalaoui (2004) a proposé une méthode d'allocation de fiabilité pour les systèmes séries-parallèles. Levitin et al. (1999) ont proposé une procédure d'optimisation basée sur la minimisation du coût total du système en considérant les taux de défaillance et de réparation des composants, et en agissant sur la fréquence de remplacement et les actions de maintenance corrective et préventive. Castro et al. (2003) ont également présenté une méthode d'optimisation de la disponibilité basée sur l'allocation de redondance et les actions de maintenance. Elegbede et al. (2003) ont développé une méthodologie d'optimisation de la disponibilité basée sur les plans d'expérience afin de paramétrer l'algorithme génétique utilisé.

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 les systèmes parallèle-série comme les systèmes à structure complexe. Nous proposons 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 (Kaufmann et al., 1975).

La section 2 de l'article est dédiée aux éléments de la norme utiles au problème de conception des SIS. La section 3 présente les réseaux de fiabilité et le calcul de la disponibilité. La section 4 concerne la méthode d'optimisation exploitée. La section 5 traite deux exemples.

2. Normes et SIS

La norme IEC 61508 (IEC, 1998) est une norme internationale qui porte plus particulièrement sur les systèmes E/E/PE (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 fixe le 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. Elle donne le SIL en fonction de sa probabilité de défaillance moyenne sur demande $\left(PFD_{avg}\right)$ pour les SIS faiblement sollicités (moins d'une sollicitation par an) ou en fonction de la probabilité de défaillance par heure $\left(PFH\right)$ pour les SIS fortement sollicités ou agissant en mode continu (cf. tableau 1).

SIL	Probabilité moyenne de défaillance à la sollicitation PFD_{avg}	Fréquence des défaillances 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	$[10^{-5},10^{-4}[$	$[10^{-9},10^{-8}[$

Tableau 1 . Niveau de SIL

Les méthodes usuelles de calcul du PFD_{avg} des SIS sont des méthodes probabilistes (IEC, 1998; IEC, 2004, Goble et al., 2005). 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.

3. Réseaux de fiabilité et disponibilité

De manière générale, un graphe permet de représenter la structure et les connexions d'un ensemble complexe en exprimant les relations entre ses éléments : réseaux de communication, réseaux routiers, circuits électriques ... (Berge 1958, Cogis 2003). Les graphes constituent donc un outil de modélisation polyvalent pour une grande variété de problèmes en se ramenant à l'étude de sommets et d'arcs.

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 *r*-graphe où *r* est le nombre maximal d'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. Un graphe peut aussi être décrit par sa matrice booléenne (appelée aussi matrice de connexion), c'est-à-dire par une matrice carrée dont les lignes et les colonnes correspondent aux sommets du graphe. Les éléments valent 1 ou 0 suivant que le couple de sommets correspondant appartient ou non à U.

Un réseau de fiabilité R défini sur un ensemble $e = \{e_1, e_2, ..., e_r\}$ 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", et une application $\Delta : U \to e$ telle que:

$$\Omega(u_j) = (S_i, S_k) \text{ et } \Omega(u_{j'}) = (S_i, S_k) \to \Delta(u_j) \neq \Delta(u_{j'})$$

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. Ainsi, plusieurs arcs peuvent correspondre à un même composant, mais il se peut qu'un arc ne corresponde à aucun composant.

La figure 1 donne un exemple de réseau de fiabilité où : $e = \{e_1, e_2, e_3, e_4\}$, $S = \{O, Z, A, B, C\}$ et $U = \{(OA)_{e2}, (OA)_{e3}, (OB), (AB), (AZ), (BC), (BZ), (CB), (ZB)\}$.

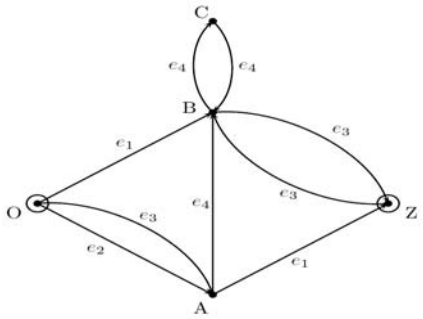


Figure 1 . Réseau de fiabilité

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

Dans un réseau de fiabilité *R*, un lien est un sous-ensemble de composants $a \subset e$ tel qu'il existe dans le graphe partiel $G_p(a)$ un chemin de *O* à *Z*. Ce graphe partiel étant le graphe *G* réduit aux arcs tel que $U_p(e_i) = \{u \in U \mid \Delta(u) \in e_i\}$. Une coupe d'un réseau de fiabilité *R* est le 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*. A toute coupe *b* du réseau correspondent une ou plusieurs coupes du graphe incluses dans $U_p(b)$. Un lien *a* (resp. coupe *b*) d'un réseau de fiabilité

est minimal si aucun sous-ensemble $a' \subset a$ (resp. $b' \subset b$) n'est un lien du réseau (resp. une coupe).

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 :

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

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.

4. Optimisation

La méthode d'optimisation choisie repose sur une méthode génétique en raison de son applicabilité à de nombreux problèmes et sa simplicité d'utilisation. Ces algorithmes ont une bonne efficacité dans la recherche d'un optimum global (Holland 1975; Goldberg 1994). En outre, ils ne requièrent pas de contrainte de monotonie, de dérivabilité de la fonction à optimiser. Ils présentent également l'avantage de proposer un ensemble de solutions optimales ou quasi-optimales.

Dans cet article, nous utilisons la méthode génétique précédemment élaborée par Bicking (1994) avec une définition particulière des chromosomes et des opérateurs appropriés de reproduction, combinaison et mutation. A partir d'une population initiale dont chaque individu représente une solution potentielle, on effectue 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.

Toutes les contraintes relatives à la définition d'un SIS comme par exemple son SIL, sont prises en comptes lors de la création des individus. Un individu est représenté par une chaîne de gènes représentant les paramètres du problème. Une correspondance entre ces chaînes et des matrices booléennes est déterminée pour construire les réseaux de fiabilité constituant également une représentation des solutions du problème.

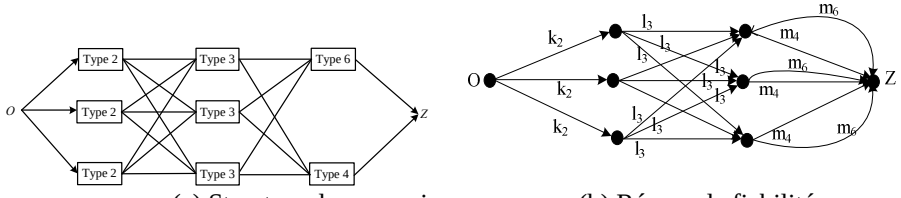
5. Études numériques

Nous utilisons une application concernant un réservoir sous pression définie dans le document technique ISA-TR84.00.02-2002 (ISA 2002). 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 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 $A_{avg} = 1 - PFD_{avg}$ 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 (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 2.

Composants du SIS	Sous-systèmes					
	Capteurs		Eléments logiques		Eléments finaux	
	Coûts	Fiabilité	Coûts	Fiabilité	Coûts	Fiabilité
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

Tableau 2 . Caractéristiques de coût et de fiabilité des composants disponibles

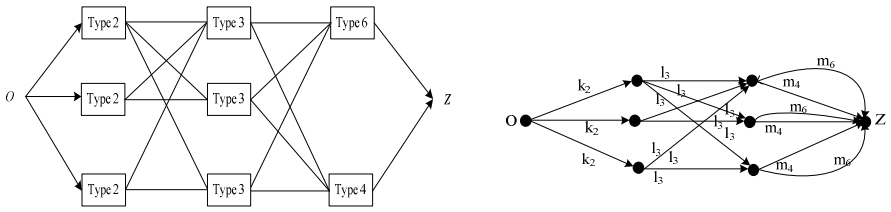
Les résultats obtenus lors d'essais pour un SIS de SIL 3 exigé conduit au SIS présenté figure 2a) et son réseau de fiabilité associé en 2b). Le coût obtenu est de 139 unités pour une disponibilité moyenne de 0,999114. Cette structure de SIS est un système série-parallèle.



(a) Structure de connexion (b) Réseau de fiabilité

Figure 2 : SIS de SIL 3 : structure (a) et réseau de fiabilité associé (b)

Si maintenant, on intègre dans le calcul du coût, le coût des connexions entre les composants (une unité par connexion), la solution trouvée lors d'essais pour un SIS de SIL 3 exigé conduit au SIS présenté figure 3a) et son réseau de fiabilité associé en 3b). Le cout est 139+13. En réduisant le nombre de connexions on aboutit à une disponibilité moyenne légèrement plus faible que le cas précédent avec une valeur de 0,999033. On constate également que cette structure de SIS n'est plus un système série-parallèle.



(a) Structure de connexion (b) Réseau de fiabilité

Figure 3 : SIS de SIL 3 : structure (a) et réseau de fiabilité associé (b)

La méthode génétique a permis également de déterminer un jeu de solutions proches de l'optimale trouvée. Ces solutions sont d'autres alternatives pour le concepteur qui peut préférer une meilleure fiabilité à coûts légèrement plus élevés.

6. Conclusion

Dans ce travail, nous avons proposé une méthodologie de détermination de structure, d'allocation conjointe de disponibilité et de redondance des composants de systèmes qui a été ensuite appliquée à la conception des SIS devant satisfaire un 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 montrent l'intérêt de la méthode employée par le fait de présenter plusieurs architectures possibles et donc d'offrir plus de choix aux concepteurs pour un même niveau de SIL donné. Comme perspectives à ce travail, nous pouvons citer l'introduction d'autres critères de sureté de fonctionnement ainsi que la prise en compte de la fiabilité des bus de communication dans les processus de conception des systèmes.

Bibliographie

Berge C., Théorie des graphes et ses applications, Dunod, France, 1958.

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

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

Cogis O. et Robert C. Théorie des graphes : Au delà des ponts de Königsberg, Problèmes, théorèmes, algorithmes, Vuibert, 2003.

Dhillon B., Design reliability: Fundamentals and applications, CRC Press LLC, 1999.

Elegbede C., Chengbin C., Adjallah K. et Yalaoui F., Reliability allocation through cost minimization, IEEE Transactions on Reliability, 52, 2003, p. 106-111.

Goble W. et Cheddie H., Safety Instrumented Systems Verification- Practical Probabilistic Calculations, ISA, 2005.

Goldberg D.E., Algorithmes génétiques Exploration optimisation et apprentissage automatique, Addison-Wesley, France, 1994.

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

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

IEC, IEC61511, Functional safety - Safety instrumented systems for the process industry sector, 2004.

Innal F., Dutuit Y. et Rauzy A., Quelques interrogations et commentaires relatifs à la norme IEC 61508, Conférence Lambda Mu 15, Lille, France, 2006.

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

Kuo W., Prasad V., Tillman F. et Hwang C., Optimal reliability design: fundamentals and applications, Cambridge University Press, 2001.

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

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

Sallak M., Simon C. et Aubry J-F., A Fuzzy Probabilistic Approach for Determining Safety Integrity Level, IEEE Transactions on Fuzzy Systems, 16(1), p. 239-248, 2008.

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

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

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