A Kaufmann reliability network approach based on components off-the-shelf to design safety instrumented systems

Christophe Simon, Frédérique Bicking, Frédéric Hamelin

Université de Lorraine, Centre de Recherche en Automatique de Nancy, UMR CNRS 7039, Vandoeuvre-lès-Nancy, F-54506, France
CNRS, Centre de Recherche en Automatique de Nancy, UMR 7039, Vandoeuvre-lès-Nancy, F-54506, France
christophe.simon;frederique.bicking;frederic.hamelin@univ-lorraine.fr

ABSTRACT. *This paper deals with an approach to design a Safety Instrumented System with the aim of reducing design costs under availability constraints. The design involves the determination of the Safety Instrumented Systems (SIS) structure and the allocation of equipment availability and redundancy based on Components off-the-shelf. The SIS structure is interpreted as a p-graph and handled as a Kaufmann reliability network. The optimization approach is genetic method applied to several design problems of increasing complexity.*

RÉSUMÉ. *Cet article développe une approche de conception de systèmes instrumentés de sécurité par une méthode d'optimisation de coût sous contraintes de disponibilité. La conception inclut la définition de la structure du Système Instrumenté de Sécurité (SIS) et l'allocation de disponibilité et de redondance à partir de composants sur étagère. La structure est vue comme un p-graphe comme l'a proposé Kaufmann. L'outil d'optimisation est un algorithme génétique qui est appliqué à plusieurs problèmes de conception de complexité croissante.*

KEYWORDS: *availability allocation; redundancy allocation; Kaufmann reliability networks; safety instrumented systems (SIS); COTS based design.*

MOTS-CLÉS : *allocation de disponibilité; redondance; réseaux de fiabilité; systèmes sntrumentés de sécurité; composants sur étagère.*

DOI:10.3166/JESA.49.449-469

1. Introduction

The application of safety standards as IEC 61508 (IEC, 1998) and sectorial standards (IEC, 2000, 2001) changes the point of view of companies about safety problems. The IEC 61508 develops a complete approach to the safety life cycle to reduce facilities' risks, and focuses on safety integrity for safety related Electrical/ Electronic/ Programmable Electronic Systems (E/E/PES) like Safety Instrumented Systems (SIS). As E/E/PES are increasingly used to perform safety functions, the IEC 61508 should be mostly applied. At the same time, many companies encountered problems with the interpretation and the application of the standards (Stavrianidis, Bhimavarapu, 2000) because they both require competencies in designing SIS and evaluating the SIS performances. SIS performance is one major key-point of the IEC 61508 standard. If the average probability of failure on demand (PFD_{avg}) is now widely recognized as an average availability, the SIS performance qualification is determined by its safety integrity level (SIL). SIS should achieve a minimum level of safety integrity defined by the SIL target based on its performance (PFD_{avg}) and the compliance with some minimum levels of fault tolerance. Fault tolerance is defined as the capacity for a system to prevent single failure escalating into system failure. It is achieved by some form of redundancy (Torres-Echeverría *et al.*, 2009a), *i.e.* hardware and software redundancies.

Another key-point in the standard is the required architecture for a SIS. The standard IEC 61508 defines some architecture conditions according to the SIL but does not define the way to design the SIS. So, some studies like (Houtermans, Rouvroye, 2005; Innal *et al.*, 2008) address the SIS architecture as a classical parallel-series system. Moreover, SIS aided design can be tackled by redundancy allocation, and most studies deal with reliability and redundancy allocations (Kuo *et al.*, 1978; Tillman *et al.*, 1980; Kuo, Prasad, 2000; Misra, 1986; Tzafestas, 2002; Coit, Smith, 1996; Yalaoui *et al.*, 2005).

In practice, there are only a limited number of different components off-the-shelf (COTS) available that can be implemented. This constraint suggests that the components of a SIS, and thus their reliability, are chosen from a discrete set. In addition to the constraint of market availability that will be taken into account in this paper, there is the issue of redundancy. The implementation of hardware redundancy implies the use of extra equipment leading to higher cost. Besides, several identical redundant components are sensitive to Common Cause Failures (CCF). One way to counteract CCF is the diversity in redundancy that means the implementation of redundancy where components are technologically different (Torres-Echeverría *et al.*, 2009b). This type of allocation of equipment reliability and redundancy has been demonstrated to be a good approach for compliance with the IEC 61508 requirements (Torres-Echeverría *et al.*, 2007). In addition, process industry uses large distance connections according to the process it handles. The cost of connections can become significant and it can be an element of cost reduction.

There are a lot of works dealing with optimization for the design of system structure integrating several factors in dependability area. For instance, (Yalaoui *et al.*, 2005) proposed a pseudo-polynomial dynamic programming method (*YCC*) based on the analogy between the reliability and redundancy allocation problem (RAP) in parallel-series systems, and a one-dimensional knapsack problem. (Elegbede *et al.*, 2003) optimizes the availability of parallel-series systems. (Castro, Cavalca, 2003) bases the optimisation problem on the maintenance factors. (Kong *et al.*, 2015) works on a new particle swarm optimisation to solve the RAP considering multiple strategies. (Coit, Smith, 1996) uses Genetic Algorithm (GA) and Neural Networks to solve the RAP of parallel-series systems with components choice. (Kuo, Prasad, 2000) addresses the same kind of problem with a search method (*PK-Alg*) based on a lexicographic order and an upper bound on the system reliability to maximize the reliability of a coherent system. (Levitin, Lisnianski, 1999) designs optimal structures at minimal costs and considers failures and repairs rates in multi-state parallel-series systems. (Torres-Echeverría *et al.*, 2009a, 2007) focuses on SIS design with RAMS and Cost constraints. It should be noticed that they introduce a diverse redundancy allocation problem (DRAP) is solved by a GA. (Bicking *et al.*, 2008) uses a GA to tackle the design of SIS layers with component choice and components interconnection with cost minimization. In (Bicking *et al.*, 2009), the same authors tackle the problem of diverse redundancy allocation and separately the definition of structure of SIS layers. (Machleidt, Litz, 2011) reduces life-cycle cost of SIS by defining K and N in KooN structures of each layer of a SIS. (Longhi *et al.*, 2015) proposes to use of NSGA-II, an elitist GA, to design SIS in a multi-objective approach with cost reduction and by working on test and repair strategies. (Innal *et al.*, 2015) considers KooN structures and uniform RAP, and introduces several parameters for the component choice. (Torres-Echeverría *et al.*, 2012) uses a multi-objective GA to reduce life-cycle cost and considers KooN structures and components choice while integrating several parameters for each kind of components.

This paper extends the previous works of the authors (Bicking *et al.*, 2008, 2009) and concerns the DRAP and cost minimization under availability and hardware fault tolerance (HFT) constraints. Contrarily to recent works, SIS are not considered as purely parallel-series or KooN systems. The components choice is based on COTS with defined costs, safety parameters, and availability and HFT constraints are considered in the optimization problem. Moreover, DRAP is tackled for the defense against common cause failures. The rest of the paper is organized as follows. Section 2 sketches useful notions of Safety Instrumented Systems. Section 3 defines the Kaufmann reliability networks basics. Section 4 presents the computer aided design method proposed and the results on less to more complex problems are presented and discussed.

2. Safety Instrumented Systems

Safety Instrumented Systems are important protection layers in the process industry. A SIS is an E/E/PES and comprises sensors, logic solvers and actuators. A SIS is

used to detect hazardous events and/or to take the process or the Entity Under Control (EUC) to a safe state when predetermined conditions are violated (cf. Fig 1). The in-

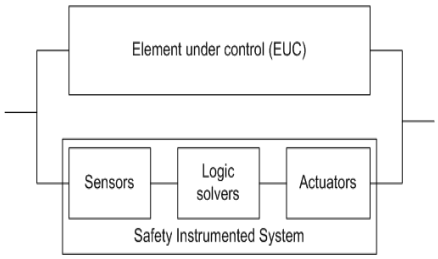

Figure 1. Implementation of the SIS with the Element Under Control

ternational standards IEC 61508 (IEC, 1998) and IEC 61511 (IEC, 2000) require that reliability targets, assigned to each Safety Integrity Function (SIF) carried out into a SIS, are defined and guaranteed. The IEC standards use safety integrity levels (SIL) as a class of performance. For a SIS operating on demand, which is often the case when the SIS is used as an independent protection layer, the average probability of failure on demand (PFD_{avg}) is computed in low demand mode or its probability to fail per hour PFH in high or continuous demand mode. According to the demand mode, the standards define SIL values presented in Table 1. In this paper, we are mostly interested in the low demand mode. The IEC 61508 (IEC, 1998), IEC 61511 (IEC, 2000) and ISA-TR84.00.02-2002 (ISA, 2002) recommend several techniques to determine the PFD_{avg}. This value is a function of the SIS configuration, the proof test interval, the common cause failures, and the inspection and maintenance policies. In the reliability research area, the PFD_{avg} of systems should be considered as an average unavailability (Innal *et al*., 2005, 2006). In this work, we use the SIS average availability A_{avg} to determine the PFD_{avg} value as follows:

$$A_{avg} = 1 - PFD_{avg} \tag{1}$$

Once the average availability A_{avg} value is obtained, we consider this value as the SIS performance even if the calculated PFD may therefore show a better performance than will be experienced in the operating phase. Because the PFD does not cover all aspects

Table 1. Definition of SIL for low and high demand modes

	Low demand	High demand
SIL	PFD_{avg}	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	$[10^{-5}, 10^{-4}]$	$[10^{-9}, 10^{-8}]$

that may cause SIS failure and to prevent SIS designers from selecting architecture based on PFD evaluations alone, some requirements on hardware architectures may be defined.

In many studies (Houtermans, Rouvroye, 2005; Langeron *et al*., 2008), SIS hardware configuration is viewed as parallel-series systems. A broader view of the SIS architecture is a three-layer system which offers more possibilities, and corresponds to many automation systems with networked control systems for instance.

Table 2. Hardware Fault Tolerance for E/E/PES

Safe Failure Fraction	Hardware Fault Tolerance (HFT)		
	0	1	2
$< 60\%$	Not Allowed	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

The SIS structure is constrained by the level of hardware fault tolerance (cf. Table 2) and the SIS performance obtained by redundancy of component or channels. A channel represents a series of sub-parts of the SIS that realises the safety function. As discussed in (Lundteigen, Rausand, 2009), this architectural constraint has been introduced because the provisional performance computed is usually over the reality. The constraint has the goal to provide more robust architectures. Nevertheless, Table 2 requires the definition of the Safe Failure Fraction (SFF) in relation with the diagnosis cover rate. (Lundteigen, Rausand, 2009) argues that SFF has not always a positive influence and (Langeron *et al*., 2007) writes that safe failure sometimes becomes dangerous. One way to make more credible the SFF value and in order to be conservative is to consider all failures as dangerous.

In conclusion, two problems are to be solved to provide a computer aided design approach of SIS based on complex architectures potentially different from parallel-series systems. They have to take into account performance targets, minimal costs and hardware fault tolerance. The first problem is to find the lower cost architecture amongst all possible architectures which respect to the required SIL constraints. The second problem is to be able to generate every kind of architectures and to compute their performance expressed by the required SIL. These problems can be formalized as an optimization problem subject to constraints. We propose to solve this problem by a genetic approach and Kaufmann reliability networks.

3. Kaufmann reliability networks (KRN)

Reliability networks are a very efficient method to compute the reliability/ availability of systems (Sahner *et al*., 1996; Colbourn, 1996; Misra, 1970; Satyanarayana, Chang, 1983; Wood, 1985; Kim, 1972). For instance, they are well-used in studies of communication networks, energy distribution networks (Rocco, Moreno, 2002), etc. Moreover, it's a competitive way to deal with the hardware structure of a system in reliability/availability optimization without structural restrictions as in usual series-parallel systems. As the goal of this work is to define the connection structure of a

SIS and to choose the components to target the necessary performance defined by the SIL, reliability networks are obviously a valuable representation to use.

As mentioned previously, the SIS architecture is a three-layer system (Fig. 1). A connection between two elements of two consecutive layers is considered as a transfer of information between the connected entities. The component failure of a layer only interrupts this transmission. In reliability block diagrams (RBD) (Guo, Yang, 2006), component failure has a different interpretation. But, a KRN can be represented as a RBD if all components of a layer transmit information to all the components of the following layer. If this is not the case, the reliability diagram is difficult or impossible to establish. Thus, any RBD can be represented by a KRN whereas some KRN cannot be represented by a RBD (cf. Fig. 3). A KRN is quite similar to a success graph as given in (Giraud, 2006). One important hypothesis in RBD is the independence between blocks. If a named block is repeated in a block diagram then the diagram is not a RBD or this is not the same block. In a KRN, a named block can be repeated without restriction that's why it is used here for this ability to easily model many structures.

3.1. Basics of KRN

Let us define some basic elements of KRN. As defined in (Kaufmann *et al.*, 1975), a reliability network is a p-graph $\mathcal{G} = \langle \mathcal{N}, \mathcal{A}, \Delta \rangle$ which consists of a set $\mathcal{N}$ of n nodes and a set $\mathcal{A}$ of a arcs. The set of arcs is defined as $\mathcal{A} \subseteq \mathcal{N} \times \mathcal{N}$. $\Delta : \mathcal{A} \mapsto \mathcal{E}$ links each arc a_{ij} to a component e_i in the set of components $\mathcal{E} = \{e_1, e_2, \ldots, e_r\}$ (Kaufmann *et al.*, 1975; Goles, Hernandez, 2000). According to Δ, more than one arc can map the same component. As the goal of arcs is to represent the system components, the nodes of the graph tie the arcs together to define the structure. The KRN $\mathcal{G}$ is acyclic and contains one source node $S \in \mathcal{N}$ with no incoming arc and one terminal node $T \in \mathcal{A}$ with no outgoing arc, also called destination or termination. A reliability network assumes that the system components e_i have binary state x_i and the system also has a binary state y as for RBD.

As mentioned in (Kaufmann *et al.*, 1975, p.79), a KRN can be a graphical representation of the structure function of a system. The structure function ϕ of a system is defined as $y = \phi(x_1, x_2, \ldots, x_r) \mapsto \{0, 1\}$. Fig. 2 shows the KRN of a system as a 1-graph which cannot be represented by a RBD when respecting the standards (Normalisation, 2006). The arcs tie the system components $\{e_1, e_2, e_3, e_4, e_5\}$ through Δ. To each component, we can assign a failure distribution by a function $P : \mathcal{E} \mapsto [0, 1]$. It is also possible to define more functions if we would assign different parameters to each component, for instance costs, repair rates, etc.

On Fig.2, we have:

- $\mathcal{N} = \{n_1, \ldots, n_9\} \, | S = n_1, T = n_9$,
- $\mathcal{A} = \{a_{12}, \ldots, a_{89}\}$,
- $\Delta : \{a_{12}, a_{15} \mapsto e_1, a_{17}, a_{23}, a_{56} \mapsto e_2, \ldots, a_{69}, a_{89} \mapsto e_5\}$.

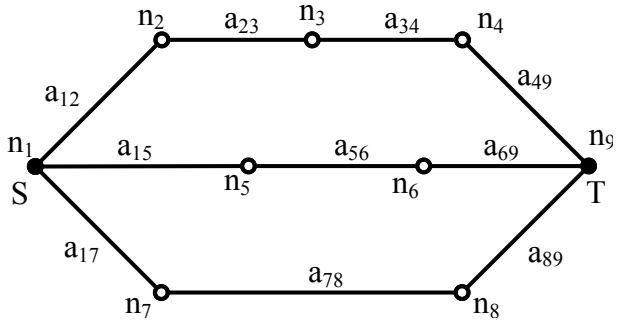

Figure 2. 1-graph of a system

The corresponding KRN is obtained by attaching to all a_{ij}, the corresponding component e_i according to Δ (see Fig. 3).

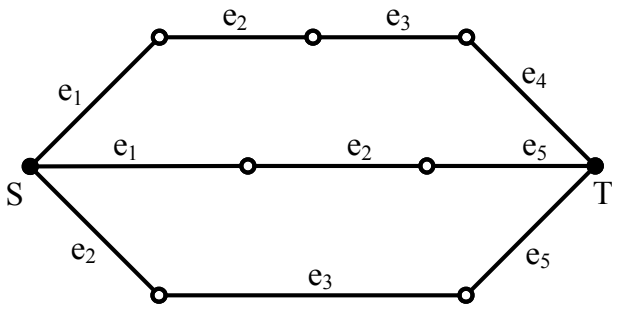

Figure 3. Corresponding KRN

A path l_i in the set of success paths $\mathcal{L}$ is a sequence of arcs linking a node $n_i \in \mathcal{N}$ to a node $n_j \in \mathcal{N}$ of the graph. l_i is elementary if it does not go twice to a same node. l_i is minimal if it has no sub-paths. In KRN, we are mainly interested in elementary paths μ_i linking S to T. The system is in up state if all arcs $a_{ij} \in \mu_i$ map components in up state. It corresponds to the strong relation between reliability networks and structure functions (Kaufmann *et al.*, 1975). A very interesting property of graphs is the equivalence between two graphs $\mathcal{G}_i$ and $\mathcal{G}_j$ if all paths in $\mathcal{G}_i$ are found in $\mathcal{G}_j$ and vice-versa (Kaufmann *et al.*, 1975, p.78). Then, a reliability network $\mathcal{G}_i$ can be rewritten in an equivalent 1-graph $\mathcal{G}_j$ as the combination of all elementary minimal paths in parallel called a success graph (Giraud, 2006). The graph in Fig.3 is initially a 1-graph and no transformation is needed. The reader can notice that it is not necessary to start with a 1-graph.

For the graph example on Fig. 2 & 3, the list of minimal paths is:

- $\mu_1 = \{a_{12}, a_{23}, a_{34}, a_{49}\} \mapsto \{e_1, e_2, e_3, e_4\}$
- $\mu_2 = \{a_{15}, a_{56}, a_{69}\} \mapsto \{e_1, e_2, e_5\}$
- $\mu_3 = \{a_{17}, a_{78}, a_{89}\} \mapsto \{e_2, e_3, e_5\}$

3.2. Computing reliability/availability

Since the success graph is obtained from the enumeration of minimal paths and is equivalent to the structure function, the reliability/availability can be computed by the inclusion-exclusion method (Misra, 1970; Kim, 1972; Lin *et al.*, 1976), the SDP (Veeraraghavan, Trivedi, 1991; Luo, Trivedi, 1998; Rai *et al.*, 1995; Soh, Rai, 1999) or factoring methods (Kim, 1972; Soh, Rai, 1999; Satyanarayana, Chang, 1983; Wood, 1985). Based on Sylvester-Poincare's theorem, the inclusion-exclusion method consists in computing the availabilty at time t by relation (2):

$$A(t) = \sum_{i=1}^{m} P(\mu_i|t) - \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} P(\mu_i.\mu_j|t) + \sum_{i=1}^{m-2} \sum_{j=i+1}^{m-1} \sum_{k=j+1}^{m} P(\mu_i.\mu_j.\mu_k|t) \quad (2)$$
$$+ \ldots + (-1)^{m+1} P(\mu_1.\mu_2.\mu_3 \ldots \mu_m|t)$$

where $P(\mu_i|t)$ is the reliability/ availability of the minimal path μ_i at time t and m is the number of minimal paths in the success graph. Please notice that availability can be computed if all events on components are independent.

The complete computation of relation (2) suffers from the exponential blow-up of the number of probability products it requires. So, this formula is essentially used for an approximation of the system reliability by keeping out the first terms of the sum with a conservative point of view.

The SDP method consists in developing the expression so that each term is an event that does not include another event of the sum, *i.e.* all the terms are disjoint (Lin *et al.*, 1976; Rai *et al.*, 1995; Veeraraghavan, Trivedi, 1991; Luo, Trivedi, 1998). The availability is then obtained by using relation (3) if the system has m minpaths:

$$A(t) = P(\mu_1|t) + P(\overline{\mu_1}.\mu_2|t) + \ldots + P(\overline{\mu_1}.\overline{\mu_2}...\overline{\mu_{m-1}}.\mu_m|t) \quad (3)$$

The computation of $A(t)$ (3) can be simplified by Abraham's method (Abraham, 1979; Heidtmann, 1989) or BDD (Rauzy *et al.*, 2003).

The SIS performance in low demand mode is not only based on individual component performance but also on the time interval of proof test T_i. For the sake of simplicity, we consider the same time of proof test $k.T_i$ for all components, and also that all failure are dangerous and, detected and repaired during the proof test. These are the hypotheses in order to use simple models like fault trees, RBD or KRN. Thus, the SIS A_{avg} can be computed on one time interval T_i and extrapolated during its mission time as follows:

$$A_{avg} = \frac{1}{T_i} \int_0^{T_i} A(t)dt \quad (4)$$

The SIS reliability R_S can be considered equal to A_{avg} because SIS in low demand mode can be considered as a non-repairable system if all the components are subject to a proof test at the same time and put in a 'as good as new' situation after test and repair. Thus, if we are able to express the structure function as a 1-graph KRN, then we are able to design a system to meet performance targets under availability constraints, tolerance to hardware failure constraint (HFT), etc.

4. Computer-aided structural design method and application

The design phase of a SIS is not particularly easy to achieve for the reliability engineer. The latter must make a choice of COTS that meet the safety requirements depending on the type of physico-chemical process, the performance level of risk reduction, architectural constraints related to standards, operating and design costs and possibly weight and volume constraints. It is possible to formalize this problem as the search for a KRN ensuring minimization of costs under different constraints by selecting components from a set of available COTS.

As mentioned before, the design problem can be considered as a minimization problem of SIS cost subjected to SIL constraints. The SIL of a SIS is characterized by its average availability (A_{avg}) over a given period defined by the test interval. The average availability, A_{avg}, is computed by relation (4).

The cost of a SIS is the sum of the costs of its components, its connections, proof tests, inspections, maintenance operations, production losses, etc. In this paper, we only address costs of components and connections. All other costs are supposed to be integrated in component costs because the more precisely we define the different costs the more precisely we should model the SIS. As our goal is to discuss the hardware configuration of SIS, the model used should be simple but powerful.

Now, the design problem is to find suitable SIS hardware configurations (*i.e.* SIS components off-the-shelf and connections among the components) that minimise the global system cost under safety integrity level constraints. This type of problem is known to be NP-hard and can be solved efficiently by meta-heuristics (Siarry, Michalewicz, 2008). Many meta-heuristics like GA, ant colony, swarm optimization, etc, can provide a solution to this problem.

4.1. Genetic method

In this article, we choose GA for optimization because they are versatile and easy to apply. GA have been demonstrated to converge to the optimal solution for many problems, although optimality cannot be guaranteed. The ability of based genetic method to find good solutions efficiently often depends on properly customizing the encoding, evolution operators and fitness measures to the specific problem. The used method is based on both genetic algorithms (Goldberg, 1989) and evolution strategies (Schwefel, 1981). It combines the principle of survival of the fittest and the structured information combination using genetic based operators to make an effective and elitist

search mechanism. Genetic method produces new solutions (child) by combining the existing solutions (parents) from a population, and by mutating the child solutions. The central idea is that superior parent solutions will tend to produce superior child solutions, so that eventually an optimal solution is obtained.

We use the genetic method previously developed in (Bicking *et al.*, 1994) with a particular definition of the chromosomes and the appropriate operators of reproduction, combination and mutation. All constraints on the definition of a SIS, such as the SIL, are taken into account in the creation of individuals. An individual is represented by a string z of genes coding the problem parameters (the components to connect and their connections from one layer to another). This individual, representing a KRN and by consequence a SIS architecture, is randomly generated according to the bounds of each gene. The population of points in the search space is generated simultaneously by contrast with the single point searched of usual optimization methods. The genetic operators improve the search process in an adaptive and elitist manner to find the global optimum. There are more complicated genetic operators but generally basic ones as well as various modifications of them can be applied. The choice of these operators depends on the nature of the problem and the performance requirements.

The mechanism can be globally sketched as follows:

1. Generate randomly a population of N individuals z_i wrt to the constraints.
2. Evaluate the fitness of all individuals in the population.
3. Test the termination criterion. If it is fulfilled then stop.
4. Select a ratio G of the best individuals (parents for the production of new individuals).
5. Combine the genetic material of the selected parents to produce a new individual.
6. Test the fitness of this new individual and the respect of constraints. If it is good then this new individual is accepted else it is destroyed and another one is generated randomly (mutation occurs with p_m) until acceptance.
7. Repeat step 4 to 6 until the population is entirely re-constructed
8. Go to step 3

Three tuning parameters are to be set. N defines the population size (usually 500), G is the population gap rate (usually 0.2), *i.e.* the number of better individuals allowed to create child for the next generation. Another parameter concerns the mutation operator which occurs with a probability p_m. Usually p_m is set to 0.1. The strategy is globally elitist to eliminate the non-adapted individuals (poor solutions) and to guarantee a sufficient genetic diversity of the population.

The principle of genetic algorithms being widely known (Holland, 1975; Goldberg, 1994), we do not develop it more in this article. However, the main effort focuses on the coding used to solve the constrained optimization problem. The first problem is to consider DRAP. The RAP is a classic problem that has been widely studied in the literature as mentioned in the introduction. In contrast, it has never been treated

by the KRN. The DRAP is more complicated than RAP, and our approach is shown to be effective to handle it. Then, the next part is dedicated to structure determination and diverse redundancy allocations.

4.2. Illustration example

To illustrate the proposed approach to find an optimal choice of SIS components and design structure under constraints, we consider the design of a SIS whose allocated SIL is imposed by the designer and the application is made with a cost minimization. Accordingly, we must determine the structure of the SIS, choose the components and their type for each subsystem of the SIS, as well as the connections among these components to obtain the required SIL. The constraint on the required SIL is transformed into a constraint on the average availability of the SIS using Table 1. The problem may be reduced to a problem of minimization of the SIS cost under the constraints of average availability (cf. Table 1) and HFT (cf. Table 2).

Let us consider that 6 component types are available off-the-shelf for each subsystem. The failure rate values and costs of SIS components available for each subsystem are given in Table 3. The failure rates of components correspond to the values used in reliability databases (Goble, Cheddie, 2005; Exida, 2005; Hauge *et al.*, 2006). The costs are arbitrarily chosen but the most important is the relative costs according to reliability. In addition, it respects the usual notion that the most reliable a component is, the most expensive it is.

Table 3. Costs and failure rate of SIS components (types 1 to 6)

Component Types	Subelements					
	Sensors		Logic elements		Actuators	
	c_1	$\lambda_1 \times 10^{-6}/h$	c_2	$\lambda_2 \times 10^{-6}/h$	c_3	$\lambda_3 \times 10^{-6}/h$
Type 1	21	7.95	14	18.86	25	21.07
Type 2	15	14.51	21	10.25	35	12.37
Type 3	20	6.09	12	14.51	41	8.16
Type 4	25	3.83	22	8.16	27	4.04
Type 5	45	2.01	26	2.01	28	6.09
Type 6	30	4.55	22	6.09	31	2.01

As previously written, the design problem is to find the optimal SIS configuration (*i.e.* SIS component types and connections among the components) under constraints such as:

$$\min Cost(z_i)$$

wrt $\underline{A_{avg}} \leq A_{avg}^{z_i} \leq \overline{A_{avg}}$ and HFT (cf. table 2)

where $\underline{A_{avg}}$ and $\overline{A_{avg}}$ are the lower and upper bounds of the average availability respectively given by Table 1, $A_{avg}^{z_i}$ is computed by (1-4). Please not that A_{avg}^{z} is computed thanks to a SIS structure corresponding to the individual z_i generated by the GA. The function $Cost(z_i)$ is the sum of the costs of components involved in z_i as given in table 3.

The method previously described is applied to design SIS under constraints. In this part, we test the method with different SIL levels required. For each experiment, the configuration of the SIS is a 3 layer system with a maximum number of components by layer equal to 6. The components of one layer have to be chosen among a list of COTS (Table 3). The structure obtained and the components chosen by the GA lead to a candidate configuration with at least 1 component per layer and at most 6 components per layer. From one extreme to another, there are other solutions, but in all cases, each configuration has got the desired SIL level and verifies the HFT. The optimization method works later on the cost minimization.

4.3. Diverse redundancy allocation problem(DRAP)

The problem here is fairly simple. It is to choose the components to be placed in each subsystem to minimize the SIS cost under the constraint of availability expressed by the SIL level and the HFT constraint. Each component is connected to all the components in the contiguous layers. The coding used in the genetic method is a string of $6 * 3 = 18$ parameters representing the types of components as follows:

$$c_{11} \dots c_{1j} \dots c_{16} c_{21} \dots c_{2j} \dots c_{26} c_{31} \dots c_{3j} \dots c_{36}$$

with:

$$c_{ij} = \begin{cases} 0, & \text{if the component is not connected} \\ k, & \text{if the connected component is of type } k \in \{1, \dots, 6\}; \end{cases}$$

4.3.1. SIL 1 required

The goal is to obtain a SIS of SIL 1 and a HFT=0. The genetic method has been ran and the result obtained is a SIS with a cost of 66 units, and a corresponding availability value of 0.90693. As the GA is a stochastic approach, the proposed method has been ran 100 times to ensure the result obtained with different genetic tuning parameter. The proposed genetic method has been tested with a population size from $N = 500$ to 1000 and the generation gap parameter $G = 0.2$ to 0.4.

The KRN obtained is depicted in Fig. 4. It can be noticed that the KRN obtained presents a classical series-parallel system which is composed of one sensor of type 2, two logic solvers of type 3 in parallel and one final element of type 4.

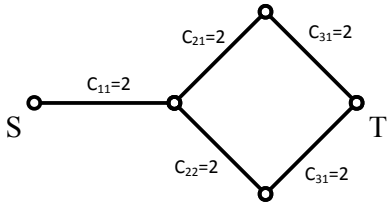

Figure 4. KRN for a SIS of SIL 1 ($A_{avg} = 0.90693$; $Cost = 66$) :

4.3.2. SIL 2 required

Now, let us considered the design objective of SIL 2 and a HFT=1. The result obtained by the GA for the SIS cost is 111 units, and the corresponding availability value is 0.991024 which corresponds to SIL2 as required (Table 1). Figure 5 shows the KRN obtained. The SIS is composed of two sensors of types 2 and 3, two logic elements of type 3 and two final elements of types 1 and 4.

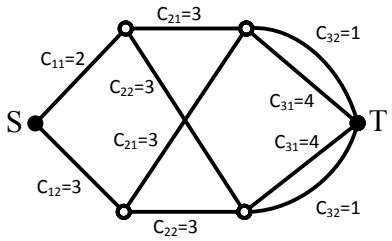

Figure 5. KRN for a SIS of SIL 2 ($A_{avg} = 0.991024$; $Cost = 111$)

4.3.3. SIL 3 required

The design objective is a SIL 3 and HFT=2. The result obtained for the SIS cost is 139 units, and the corresponding availability value is 0.9991142 which corresponds to SIL3. Figure 6 shows the KRN found. The SIS is composed of three sensors of type 2, three logic elements of type 3 and three final elements of types 6 and 4.

4.3.4. SIL 4 required

The goal is a SIL 4 and HFT=2. We obtain a SIS configuration which satisfies the required SIL with $A_{avg} = 0.99990499$, and a minimal cost of 184. Fig. 7 shows the KRN obtained. The SIS is composed of three sensor of types 3 and 2, four logic elements of type 3 and three final elements of type 4. In these experiments, we get other configurations with a cost and a reliability slightly higher thanks to the GA approach used. An example of one of these configurations is a SIS defined by the following gene $x = [002043333100400404]$. It means the SIS is composed of 3 sensors (types 2, 3 and 4), 4 logic elements (types 1 and 3) and 3 final elements (type 4). The cost of this SIS is $C = 191$ units and the average availability is $A_{avg} =$

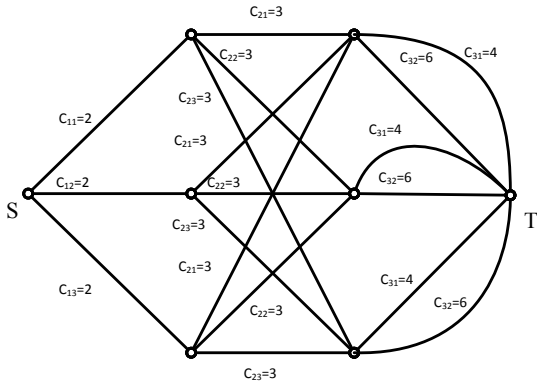

Figure 6. KRN of a SIS for SIL3 ($A_{avg} = 0.9991142$; $Cost = 139$)

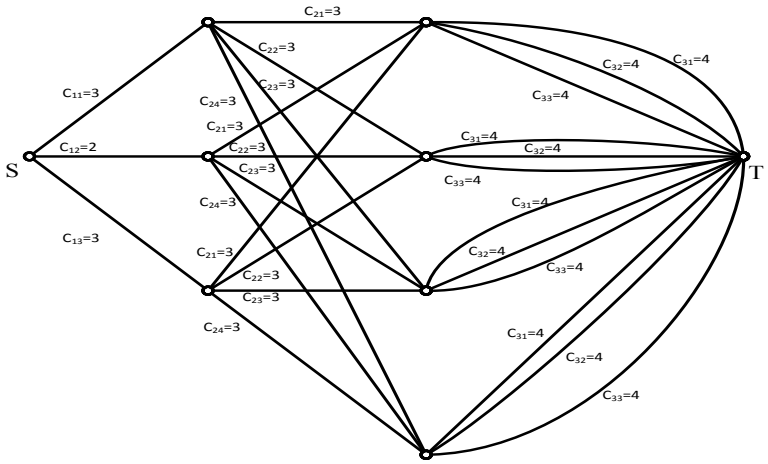

Figure 7. KRN for a SIS of SIL4 ($A_{avg} = 0.99990499$; $Cost = 184$)

0.99992123. The other most interesting configurations obtained are summarized in Table 4.

Table 4. Average availability and costs values for other SIS of SIL 4

SIL	code structure	cost	average availability
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

4.4. Discussion

These experiments show that the design of a SIS by the minimization of the cost under SIL constraints incorporating diverse redundancy and based on COTS is feasible. However, some comments should be made. The cost definition of the SIS is fairly simple. But, it can be improved by including other costs like production loss, fixed maintenance costs or variable maintenance costs regarding component types, etc. In the same idea, system availability can be revisited. The hypotheses made for computing the average probability of failure on demand can be considered too restrictive. Several proof test intervals, coverage diagnostic rates, repairs during operation, SFF can be introduced in the problem but it probably rejects the KRN modeling approach.

Diverse redundancy intuitively reduces the common cause failure because components are of different types and not sensitive to the same factors. But, CCF is hard to value. So, it is difficult to integrate it in the optimisation process until it is valued, but it can integrate the constraints *i.e.* by requesting the diversity. One can try to integrate common cause failure models like the model of factor β (Fleming, 1974), the PDS method (Hauge *et al.*, 2006), the model of Multiple Greek Letters (MGL) (Barros *et al.*, 2009) or the model of factor α (Vaurio, 2007). β- model is quite easy to use but the remaining question is how to value its parameters in the case of diverse redundancy.

Thanks to a GA approach, some arrangements can be designed to maximize the probability of successful operation (reliability or availability) and lead to different architectures that are no longer necessarily parallel-series, but depend on how the various components are connected. This work is the subject of the following section.

4.5. Search of the SIS architecture

The problem we handle here is the simultaneous search of the COTS and how to connect them to meet the performance of risk reduction with a minimal cost. The cost of connection makes sense in terms of cost due to the connectors in the process industry, while the operational cost is transferred onto the component costs.

As in the previous case, our goal is to design a SIS with a required SIL. So, it is necessary to determine the SIS structure, to choose the components and their types for each subsystem of the SIS, as well as the connections among these components to obtain the required SIL with a minimal cost. The constraint on the required SIL is transformed into a constraint on the average availability of the SIS using Table 1. The problem can be reduced to a problem of minimizing the overall cost of the SIS under the constraint of its average availability computed from equation (4). The overall cost of the SIS is the sum of the costs of its components including purchase costs and operational costs of the connections among components defined as one unit per connection. The characteristics of the components used are given in Table 3.

The coding used is a string of 102 parameters representing the types of components and their connections from a sub-system to another as follows:

$$c_{11} \dots c_{16} c_{21} \dots c_{26} c_{31} \dots c_{36} l_1 \dots l_6 l_7 \dots l_{42} l_{43} \dots l_{78} l_{79} \dots l_{84}$$

This code is defined for up to 6 components by layers and all possible connections between layers' components. $l_1 \dots l_6$ are binary values coding the links between the source S and the components of the sensor layer and $l_{79} \dots l_{84}$ encode those components of the final layer to the terminal T. The values $l_7 \dots l_{42} l_{43} \dots l_{78}$ encode the existence of a link between a component of a layer and the components belonging to the successive layer. Thus, if all values of l_i are equal to one, the SIS structure is fully connected and it boils down to a series-parallel system.

The optimization algorithm is performed with the new definition of the SIS structure coding. The solution found in tests for SIS with a required SIL 3 led to the KRN in Fig. 8. The SIS structure obtained is not a parallel-series system. The cost is $139 + 13 = 152$ units and the average availability is $A_{avg} = 0.999033$. Reducing the number of connections would lead to an average availability slightly lower than in the previous case where $A_{avg} = 0.999114$ with a parallel-series system (cf. Section 4.3.3).

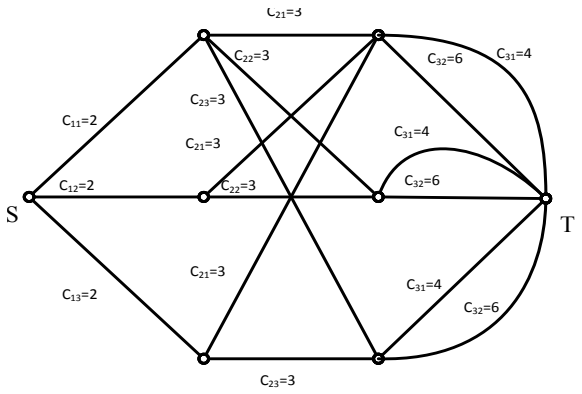

Figure 8. KRN for a SIS of SIL3 ($A_{avg} = 0.999033$; $Cost = 152$)

The solution found in tests for SIS with a required SIL 4 leads to the SIS presented in Fig. 9. The SIS structure obtained is not a parallel-series system. The cost is 204 units and the average availability is $A_{avg} = 0.999963$. We can observe that the redundancy is homogeneous but the connections of components lead to an atypical structure of the SIS as it cannot be drawn with a RBD.

4.6. Discussion

In the IEC 61508, there is no notion of cost. Everybody knows the sentence *Safety has no price*, but it is false. So, if for safety reasons the analyst would increase the redundancy, he/she would naturally connect each component of one layer to each

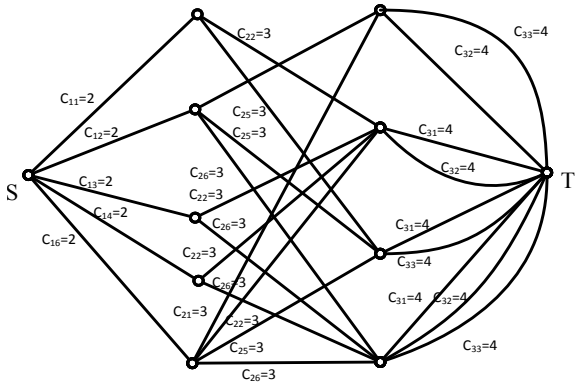

Figure 9. KRN for a SIS of SIL 4 ($A_{avg} = 0.999963$; $Cost = 204$)

of its following layer. It makes sense if one accepts the cost and the reliability of connections.

By considering the cost of connection and the possibility of programmable systems, it is possible to use not totally interconnected layers as previously proposed. Compared with the structure proposed in (IEC, 1998) and (Houtermans, Rouvroye, 2005), it is quite unusual.

Concerning the diverse redundancy as exhibited between the logic solver layer and the actuator layer of the SIS in Fig. 8, it is also unusual (see. IEC (1998); Houtermans, Rouvroye (2005)). When the analyst attempts to solve the performance problem, he uses components that functionally answer to the safety problem and then chooses the level of redundancy. It is a bit complicated to try solving the optimization problem by hand. When introducing the possibility of diverse redundancy, the valuation of the common cause failure is more complicated than in the uniform redundancy case. The β-factor model is typically in that sense of simplicity. At least, the HFT constraint is not so easy to introduce and to take into account in the hand made design of a SIS.

5. Conclusion

In this paper, we formulated an original approach based on KRN for availability and diverse redundancy allocation. This approach was used for the optimal design of SIS to achieve a required SIL with cost minimization based on COTS and HFT constraint. A primary interest of the methodology is to lead to structures where the redundancy is not uniform which reduces intuitively the importance of risk of common cause failure even if it is not the direct objective of this work. The second interest is to obtain configurations that are not conventional series-parallel architectures that make sense in cost reduction when connection costs become significant. By using KRN as system modeling, the reliability of any three-layer structure can be computed. A third interest of the methodology is to present several possible architectures and thus offer more design choices according to other criteria not defined in the specifications.

We are also able to introduce different constraints for particular problems like weight, size, etc, usually encountered in embedded systems for instance.

Further research should focus on taking into account reliability of connections, failure dependencies, failure modes and periodic inspections. Finally, we can state that the proposed model remains open to the integration of elements that have not been modeled here such as the common cause failure rates, the diagnostic coverage, the proof-test interval, the operating and maintenance costs, etc.

References

Abraham J. (1979). An improved algorithm for network reliability. *IEEE Transactions on Reliability*, Vol. 28, pp. 58-61.

Barros A., Grall A., Vasseur D. (2009). Estimation of common cause failure parameters with periodic tests. *Nuclear engineering and Design*, Vol. 239, No. 4, pp. 761-768.

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

Bicking F., Simon C., Aubry J.-F. (2008). Aide à la conception de systèmes instrumentés de sécurité. In *16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda Mu 16*, p. CDROM. Avignon, France.

Bicking F., Simon C., Sallak M., Aubry J.-F. (2009). Aide à la conception de Systèmes Instrumentés de Sécurité par les réseaux de fiabilité de Kaufmann. In *2ème Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes, 3SGS'09*, p. CDROM. Nancy, France.

Castro H., Cavalca K. (2003). Availability optimization with genetic algorithm. *International Journal of Quality and Reliability Management*, Vol. 20, pp. 847-863.

Coit D., Smith A. (1996). Solving the redundancy allocation problem using a combined neural network/genetic algorithm approach. *IEEE Computer and Operation Research*, Vol. 23, pp. 515-526.

Colbourn C. (1996). *The combinatorics of networks reliability*. Oxford University Press.

Elegbede C., Chengbin C., Adjallah K., Yalaoui F. (2003). Reliability allocation through cost minimization. *IEEE Transactions on Reliability*, Vol. 52, pp. 106-111.

Exida (Ed.). (2005). *Safety equipment reliability handbook, 2nd edition*. Exida.

Fleming F. (1974). A reliability model for common mode failures in redundant systems. *GA-A-13284*.

Giraud M. (2006). Sûreté de fonctionnement des systèmes: Analyse des systèmes non réparables. In *Techniques de l'ingénieur.* Techniques de l'ingénieur.

Goble W., Cheddie H. (2005). *Safety instrumented systems verification: practical probabilistic calculations*. ISA.

Goldberg D. (1989). *Genetic algorithms in search, optimization, and machine learning*. Addison-Wesley.

Goldberg D. (1994). *Genetic algorithms*. Addisson-Wesley.

Goles E., Hernandez G. (2000). Dynamical behavior of kauffman networks with and-or gates. *Journal of Biol. Systems*, Vol. 8, pp. 151-175.

Guo H., Yang X. (2006). A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety*, Vol. 92, pp. 1267-1273.

Hauge S., Hokstad P., Langseth H., Oien K. (2006). *Reliability prediction method for safety instrumented systems*. SINTEF.

Heidtmann K. (1989). Smaller sums of disjoint products by subproduct inversion. *IEEE Transactions on Reliability*, Vol. 38, pp. 305-311.

Holland J. H. (1975). *Adaptation in natural and artificial systems*. University of Michigan Press.

Houtermans M., Rouvroye J. (2005). *The influence of design parameters on the probability of failure on demand (pfd) performance of safety instrumented systems (sis)*. Technical report.

IEC. (1998). *Iec 61508. functional safety of electrical/electronic/programmable electronic (e/e/pe) safety related systems.*

IEC. (2000). *Iec 61511. functional safety: Safety instrumented systems for the process industry sector.*

IEC. (2001). *Iec 61513. nuclear power plants - instrumentation and control for systems important to safety - general requirements for systems.*

Innal F., Dutuit Y., Chebila M. (2015). Safety and operational integrity evaluation and design optimization of safety instrumented systems. *Reliability Engineering & System Safety*, Vol. 134, pp. 32 - 50.

Innal F., Dutuit Y., Djebabra M. (2005). An analysis of simplified equations in cei 61508-6. In *Proceedings of the qualita 2005 conference, bordeaux, france.*

Innal F., Dutuit Y., Rauzy A. (2006). Some interrogations and remarks about cei 61508. In *Proceedings of the lambda mu 2006 conference, lille, france.*

Innal F., Dutuit Y., Rauzy A., Signoret J.-P. (2008). *New insight into pfdavg and pfh, safety users group*. Technical report.

ISA. (2002). *Isa-tr84.00.02-2002. safety instrumented fonctions (sif), safety integrity level (sil), evaluation techniques.*

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

Kim Y. (1972). A method for computing complex system reliability. *IEEE Transactions on Reliability*, Vol. 21, pp. 215-219.

Kong X., Gao L., Ouyang H., Li S. (2015). Solving the redundancy allocation problem with multiple strategy choices using a new simplified particle swarm optimization. *Reliability Engineering & System Safety*, Vol. 144, pp. 147 - 158.

Kuo W., Hwang C., Tillman F. (1978). A note on heuristic methods in optimal system reliability. *IEEE Transactions on Reliability*, Vol. 27, pp. 320-324.

Kuo W., Prasad V. (2000). Reliability optimization of coherent systems. *IEEE Transactions on Reliability*, Vol. 49, pp. 323-330.

Langeron Y., Barros A., Grall A., Bérenguer C. (2007). Safe failure impact on safety instrumented systems. In T. Aven, J. Vinnem (Eds.), *Proceeding of the safety and reliability conference, esrel'07*, Vol. 1, pp. 641–648.

Langeron Y., Barros A., Grall A., Bérenguer C. (2008). Combination of safety integrity levels (sils): A study of iec61508 merging rules. *Journal of Loss Prevention in the Process Industries*, Vol. 21, pp. 437-449.

Levitin G., Lisnianski A. (1999). Joint redundancy and maintenance optimization for multistate series-parallel systems. *Reliability Engineering and System Safety*, Vol. 64, pp. 33-42.

Lin P., Leon B., Huang T. (1976). A new algorithm for symbolic system reliability analysis. *IEEE Transactions on Reliability*, Vol. 25, pp. 2-15.

Longhi A. E. B., Pessoa A. A., Almada Garcia P. A. de. (2015). Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. *Reliability Engineering & System Safety*, Vol. 142, pp. 525 - 538.

Lundteigen M., Rausand M. (2009). Architectural constraints in iec 61508: Do they have intended effects? *Reliability Engineering and System Safety*, Vol. 94, pp. 520-525.

Luo T., Trivedi K. (1998). An improved algorithm for coherent system reliability. *IEEE Transactions on Reliability*, Vol. 47, pp. 73-78.

Machleidt K., Litz L. (2011, Jan). An optimization approach for safety instrumented system design. In *Reliability and maintainability symposium (rams), 2011 proceedings - annual*, p. 1-6.

Misra K. (1970). An algorithm for the reliability of redundant networks. *IEEE Transactions on Reliability*, Vol. 19, pp. 146-151.

Misra K. (1986). *On optimal reliability design: a review*. System Science.

Normalisation A. F. de. (2006). *NF EN 61078 - techniques d'analyse pour la sûreté de fonctionnement - bloc-diagramme de fiabilité et méthodes booléennes*. Technical report No. NF EN 61078. AFNOR.

Rai S., Veeraraghavan M., Trivedi K. (1995). A survey of efficient reliability computation using disjoint products approach. *IEEE Networks*, Vol. 25, pp. 147-163.

Rauzy A., Chatelet E., Dutuit Y., Bérenguer C. (2003). A practical comparison of methods to assess sum-of-products. *Reliability Engineering and System Safety*, Vol. 79, pp. 33-42.

Rocco C., Moreno J. (2002). Network reliability assessment using celluler automata approach. *Reliability Engineering and System Safety*, Vol. 78, pp. 289-295.

Sahner R., Trivedi K., Puliafito A. (1996). *Performance and reliability analysis of computer system*. Kluwer Academic Publishers.

Satyanarayana A., Chang M. K. (1983). Network reliability and the factoring theorem. *Networks*, Vol. 13, pp. 107-120.

Schwefel H. (1981). *Numerical optimization of computer models*. Editions Wiley.

Siarry P., Michalewicz Z. (2008). *Advances in metaheuristics for hard optimization*. ser. Natural Computing Series, Springer.

Soh S., Rai S. (1999). Computer aided reliability evaluator for distributed computing networks. *IEEE Transactions on Parallel and Distributed Systems*, Vol. 2, pp. 199-213.

Stavrianidis P., Bhimavarapu K. (2000). Performance-based standards: safety instrumented functions and safety integrity levels. *Journal of Hazardous Materials*, Vol. 71, pp. 449-465.

Tillman F., Hwang C.-L., Kuo W. (1980). *Optimization of system reliability*. Marcel Dekker.

Torres-Echeverría A., Martorell S., Thompson H. (2007). Optimization of rams+c for a safety-instrumented system design diverse redundancy. In *Proceedings of esrel conference, stavanger, norway.*

Torres-Echeverría A., Martorell S., Thompson H. (2009a). Design optimization of a safety-instrumented system based on rams+c addressing iec 61508 requirements and diverse redundancy. *Reliability Engineering and System Safety*, Vol. 94, pp. 162-179.

Torres-Echeverría A., Martorell S., Thompson H. (2009b). Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering and System Safety*, Vol. 94, pp. 838-854.

Torres-Echeverría A., Martorell S., Thompson H. (2012). Multi-objective optimization of design and testing of safety instrumented systems with moon voting architectures using a genetic algorithm. *Reliability Engineering & System Safety*, Vol. 106, pp. 45 - 60.

Tzafestas S. G. (2002). Optimization of system reliability: A survey of problems and techniques. *International Journal System Science*, Vol. 11, pp. 455-486.

Vaurio J. K. (2007). Consistent mapping of common cause failure rates and alpha factors. *Reliability Engineering & System Safety*, Vol. 92, No. 5, pp. 628 - 645. (Recent Advances in Theory & Applications of Stochastic Point Process Models in Reliability Engineering)

Veeraraghavan M., Trivedi K. (1991). An improved algorithm for symbolic reliability analysis. *IEEE Transactions on Reliability*, Vol. 40, pp. 347-358.

Wood R. (1985). A factoring algorithm using polygontochain reductions for computing k-terminal network reliability. *Networks*, Vol. 15, pp. 173-190.

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

Article soumis le 5 mai 2015
Accepté le 7 octobre 2015