OPTIMAL DESIGN OF SAFETY INSTRUMENTED SYSTEMS: A GRAPH RELIABILITY APPROACH

SALLAK Mohamed* – SIMON Christophe – AUBRY Jean-François***

Centre de Recherche en Automatique de Nancy, Nancy Université, CNRS UMR 7039
* ENSEM, 2 Avenue de la forêt de Haye,
54506, Vandoeuvre-Les-Nancy, France
Tél : 33 (0)3.83.59.56.47
Fax : 33 (0)3.83.59.56.44
mohamed.sallak@ensem.inpl-nancy.fr
jean-françois.aubry@isi.u-nancy.fr
** ESSTIN, 2 Rue Jean Lamour,
54519, Vandoeuvre-Les-Nancy, France
Tél : 33 (0)3.83.68.51.34
Fax : 33 (0)3.83.68.50.01
christophe.simon@esstin.uhp-nancy.fr

Mots clés : Systèmes Instrumentés de Sécurité, Niveaux d'Intégrité de Sécurité, conception optimale, structure optimale, réseaux de fiabilité, algorithmes génétiques.

Key words: Safety Instrumented Systems (SIS), Safety Integrity Level (SIL), optimal design, optimal structure, reliability graphs, genetic algorithms.

Thème: Fiabilité, maintenabilité, disponibilité.

Résumé : Les Systèmes Instrumentés de Sécurité (SIS) sont des systèmes qui ont pour objectif de mettre un procédé industriel en position de repli de sécurité lorsqu'il évolue vers un comportant à risque réel pour le personnel et l'environnement. Pour concevoir ces systèmes, deux normes sont utilisées : l'ANSI/ISA S84.01-1996 et l'IEC 61508. Cependant, les fiabilistes ont beaucoup de difficultés à mettre en oeuvre les prescriptions de ces deux normes, notamment pour la conception des SIS dont on exige un niveau d'intégrité de sécurité (SIL) donné. A notre connaissance, le problème de conception optimale des SIS à structure indéfinie et avec un choix réduit de composants n'a pas été traité auparavant. Cet article propose une approche basée sur les réseaux de fiabilité et les algorithmes génétiques pour la conception optimale des SIS. En guise d'illustration, le modèle est appliqué à la conception d'un SIS qui doit implémenter une Fonction Instrumentée de Sécurité de SIL 1 avec un coût minimal et un choix réduit de composants.

Abstract: A Safety Instrumented System (SIS) is designed for the purpose of mitigating a risk or bringing the process to a safe state in the case of a process failure. However, in the field there is a considerable lack of understanding how to apply the ANSI/ISA S84.01-1996 and IEC 61508 safety standards in order to design SIS to meet the required Safety Integrity Level (SIL). Since no existing study has analyzed the optimal design of SIS with undefined structure and components choice constraints, this paper presents an optimization approach using reliability graph and genetic algorithm to identify the choice of components and design configuration in a SIS. An example which illustrates the use of the proposed approach to achieve a SIL 1 under cost and components choice constraints is proposed.

1 – Introduction

The process industry tends to be technically complex and has the potential to inflict serious harm to people and goods during a spurious trip. Experiences gained from accidents have led to the application of a variety of systems, such as Safety Instrumented Systems (SIS). The SIS is a system designed for the purpose of mitigating a risk or bringing the process to a safe state in the case of a process failure. The ANSI/ISA S84.01-1996 [ISA] and IEC 61508 [IEC 61508] safety standards provide guidelines for the design, installation, operation, maintenance and test of SIS. According to these standards, the Safety Integrity Level (SIL) of a SIS is defined by its average probability to fail on demand PFD_{avg}. However, in the field there is a considerable lack of understanding how to apply the safety standards in order to design SIS to meet the required SIL. The use of redundant components increases the SIL level, but it also increases the design cost. Therefore, optimization methods are necessary to determine reliability and redundancy allocation in a SIS, in order to minimize the SIS cost fulfilling constraint of SIL.

In most of the studies on reliability and redundancy allocation [Kuo & Prasad 00] [Misra 86], the reliability of the components may be any real between 0 and 1. In practice, only few different components that may be used in a SIS are available in the market, and this assumption is rarely considered. Coit and Smith [Coit & Smith 96] presented an optimization approach using a genetic algorithm (GA) with a neural network to identify the choice of components and design configuration in a series - parallel system. Kuo and Prasad [Kuo et al. 01] presented a search method (PK-Alg) based on lexicographic order to maximize the reliability of a coherent system over component choices and redundancy options. Yalaoui et al. [Yalaoui et al. 05] proposed a dynamic programming method (YCC) based on the analogy between the reliability and redundancy allocation problem in parallel - series systems, and a one-dimensional knapsack problem. This method takes into account the market constraints. Since no existing study has analyzed the optimal design of SIS with undefined structure and components choice constraints, this paper presents an optimization approach using reliability graph and genetic algorithm to identify the choice of components and design configuration in a SIS with undefined structure.

This paper is organized as follows. Section 2 briefly describes SIS and reliability methods to evaluate the SIL level. Then the reliability graph method is introduced to evaluate the SIL of the SIS. Section 3 formulates the problem of optimal design of SIS. Then a genetic algorithm is developed to solve this problem in section 4. Section 5 concerns a simple example which illustrates the use of the proposed approach and effectiveness of our algorithm. Finally, some concluding remarks and perspectives are given in Section 6.

2 – Safety Instrumented Systems (SIS) and reliability graphs

2.1 – Safety Instrumented Systems

The SIS is a system composed of three layers: sensors, logic solver and final elements for the purpose of taking the process to a safe state when predetermined conditions are violated (cf. Figure 1).

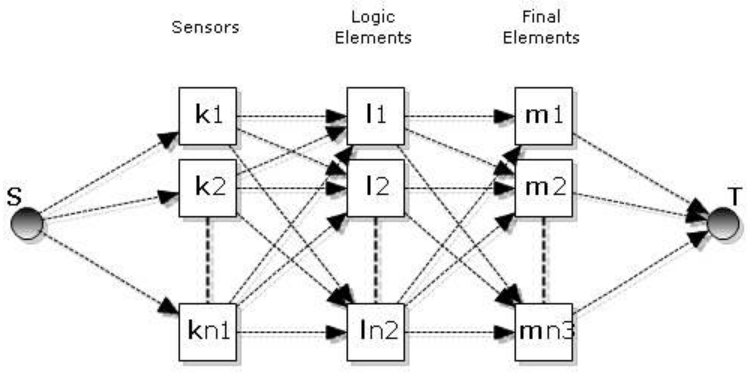

Figure 1: Reliability block diagram of SIS

The safety performance of the SIS is defined in terms of SIL, which is defined by the average probability to fail on demand (PFD_{avg}) over a given time period. For safety functions with a low demand rate and

safety functions with a high demand rate, the ANSI/ISA S84.01-1996 [ISA] and IEC 61508 [IEC 61508] standards use Table 1.
In order to evaluate the SIL of SIS, the safety standards [IEC 61508] [ISA] propose three quantitative methods to determine the PFD_{avg} value:

- Simplified equations.
- Fault tree analysis.
- Markov modelling.

Tableau 1: Definition of SIL for low and high demand modes.

Demand mode	Low	High
SIL	PFD_{avg}	Failures/hour
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	$[10^{-5};10^{-4}[$	$[10^{-9};10^{-8}[$

In many of reliability allocation problems, the optimization methods use reliability block diagram to represent series parallel structures. In this paper, we aim to obtain optimal configurations of systems with undefined struture (not only series parallel structures), that's why we use reliability graph method defined by Kaufmann et al. [Kaufmann et al. 77] to represent and study these systems.

2.2 – Reliability graph method

A very efficient method to compute the reliability of a system is to express it as a reliability graph [Sahner et al. 96] [Kaufmann et al. 77]. This method is particularly attractive for system reliability analysis due to its intuitiveness.

The reliability graph model G consists of a nonempty set $N(G)$ of nodes, a set $E(G)$ of arcs, and an incidence relation. For each arc of G, the incidence relation associates a pair of nodes of G, called its ends, where the arcs represent components that can fail. The graph contains one source node (S) with no incoming arcs and one sink node (T), also called destination or termination, with no outgoing arcs. A system represented by a reliability graph fails when there is no path from the source to the sink. We can assign failure probabilities, failure rates or reliability values to arcs. A path is defined as a set of arcs so that if these arcs are all up, the system is up. A path is minimal if it has no proper subpaths. The minpaths is the set of all minimal paths. A cut is defined as a set of arcs so that if these arcs are all down, the system is down. A cut is minimal if it has no proper subcuts. The mincuts is the set of all minimal cuts.

Conventionally, two classes of methods are often used for reliability graph analysis. One is the factoring algorithm [Misra 70] [Satyanarayana & Chang 83]. The idea is to choose an arc and break down the model into two cases: the first assumes the component has failed, the second assumes it has not failed. For each case, a new reliability graph is built by taking into account the behavior of the chosen arc. The alternative class of methods is to directly obtain minpaths or mincuts. The inclusion-exclusion [Misra 70] [Kim et al. 72] or sums of disjoint products (SDP) [Rai et al. 95] [Veeraraghavan & Trivedi 91] methods have to be applied to obtain correct reliability expressions. In this paper, we propose to evaluate the SIL of a SIS by a reliability graph.

3 – Problem statement

In this section, notations and assumptions are first introduced; then the targeted constrained optimization problem is formulated.

3.1 – Notations

$R(x) = 1 - PFD_{avg}$ SIS average reliability
$C(x)$ SIS cost

R_{min} constraint of minimum SIS average reliability
C_{max} constraint of maximum cost
s number of subsystems in the SIS
i index of subsystem
i=1: subsystem sensors (k)
i=2: subsystem logic elements (l)
i=3: subsystem final elements (m)
j index of component type
n_i number of components types available in subsystem i
r_{ij} reliability of component type j used in subsystem i
c_{ij} cost of component type j used in subsystem i
x SIS configuration vector
$f(x)$ value of the objectif function (fitness)
1, 2, 3, ... node numbers in reliability graph

3.2 – Assumptions

- The structure function of the SIS is s-coherent (the system reliability increases with component reliability and each component is relevant).
- The SIS involves s-independent subsystems.
- The SIS and its components can only be expressed in two states: failed or operational.
- The failure properties of SIS components are only considered.
- The overall SIS cost is the sum of individual sub-system costs.
- The cost and failure probabilities of SIS components are fixed and known.
- The failure probabilities represent the average failure probabilities on demand over a period test interval.

3.3 – Problem formulation

The initial structure of a SIS can be represented by the RBD of the Figure 1. The SIS is divided into 3 subsystems (Sensors, Logic Elements and Final elements). In subsystem i, there are n_i available components types to be chosen.
Then, we convert the RBD to a reliability graph (cf. Figure 2). In this graph, arcs represent the components. Nodes represent the connections between components.

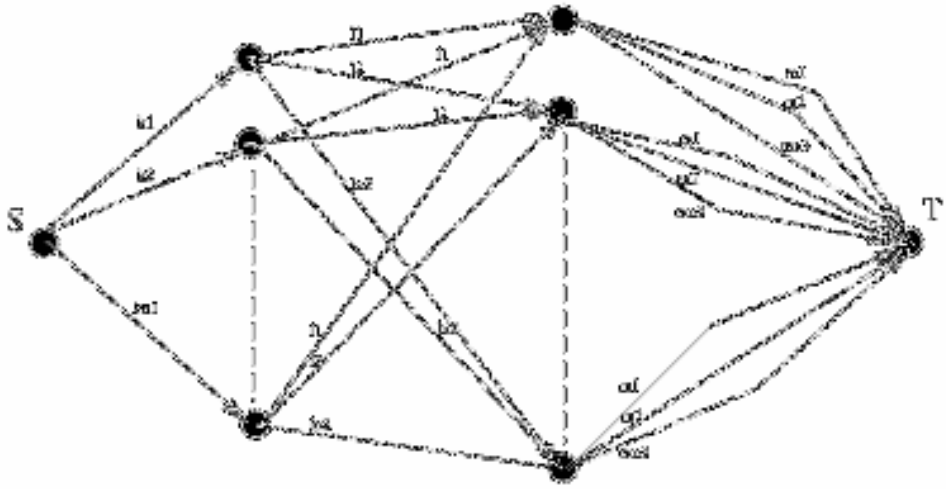

Figure 2: Reliability graph of SIS

The SIS reliability graph can thus be represented as a vector:
$x = [k_1, k_2,..., k_{n1}, l_1, l_2,..., l_{n2}, m_1, m_2,..., m_{n3}]$.
For example, the element k_1 is equal to 1 if there is an arc from nodes *S* to *1*, and *0* else. The system PFD_{avg} is then computed by enumerating minpaths of reliability graph configuration and applying SDP method to obtain the SIS reliability. The total system cost is the sum of components cost obtained in the optimal structure.

The formulation of the SIS optimization design is aimed at selecting what type of components to use in each subsystem in order to minimize the SIS cost given a required SIL for the SIS. The problem can be formulated as:

- Minimize C(x)
- Subject to: $0.9 \le R(x) \le 0.99$ (i.e., the SIL of SIS is 1).

  $C(x) \le C_{\max}$.

The objective function is the sum of the total cost for all arcs in the reliability graph plus a quadratic penalty function for reliability graph which fail to meet the minimum reliability requirement. The fitness function is:

$$f(x) = C(x) + \delta(c_{\max}(R(x) - R_{\min})^2).$$

$$\delta = \begin{cases} 1 & if \quad R(x) \le R_{\min} \\ 0 & else. \end{cases} \quad \text{and} \quad c_{\max} = \max_{i,j}\{c_{ij}\}$$

4 – Genetic algorithm implementation

4.1 – Introduction

Genetic algorithms (GAs) are usually used as an optimization technique with good efficiency to search for the global optimum of a function. The GAs were developed by John Holland [Holland 75] and further described by Goldberg [Goldberg 89]. The implementation of the GAs consists in creating an initial population with a given size (number of individuals). Then by a selection process which is defined by an adaptation function, the second step is to select the individuals who will be crossed. Then a current population is created by crossing of the individuals. The passage from a current population to another is called a generation. For each generation, the algorithm keeps the individual with the best criterion value. Recently, an increasing number of GA applications have been presented to solve the reliability optimizations, see e.g. [Coit & Smith 96] [Kumar et al. 95] [Painton & Campbell 95].

4.2 – Solution encoding

When applying GA to optimize the SIS design, an important aspect is the encoding of the potential solutions. In a general way, a potential solution (a chromosome) is a configuration of the SIS reliability graph. The encoded variables are, therefore, the arcs (components) between reliability graph nodes. In that sense, each chromosome *x* is coded through a vector consisting of several genes. Each gene x_{ij} is equal to one if there is an arc between nodes *i* and *j*, and *0* else. Figure 3 shows a reliability graph composed of *4* nodes and *3* arcs present. The chromosome *x* is defined as:
$x = [x_{S1}\ \ x_{S2}\ \ x_{1T}\ \ x_{3T}] = [1\ \ 1\ \ 1\ \ 0]$.

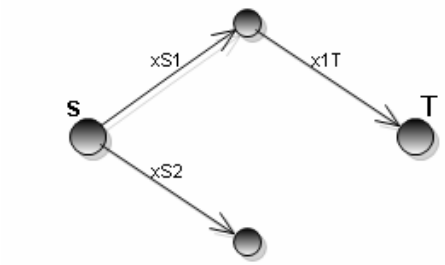

Figure 3: A reliability graph

4.3 – GA parameters

The choice of parameters for GA can affect performance of the algorithm. These parameters include population size, crossover rate and mutation rate. There have been many different studies to find the optimal control parameters [Costa et al. 05]. Instead, we run a set of experiments to establish parameter values which work well and to gauge the sensitivity of the GA to alterations in those values.

5 – Application example

In order to illustrate the proposed approach, let us consider a process composed of a pressurized vessel containing volatile flammable liquid (see Figure 4). The example process and the SIS are defined in ISA-TR84.00.02 [ISATR]. The engineered systems available are:

- An independent pressure transmitter to initiate a high pressure alarm and alert the operator to take an appropriate action to stop inflow of material.
- In case the operator fails to respond, a pressure relief valve releases material in the environment and thus reduces the vessel pressure and prevents its failure.

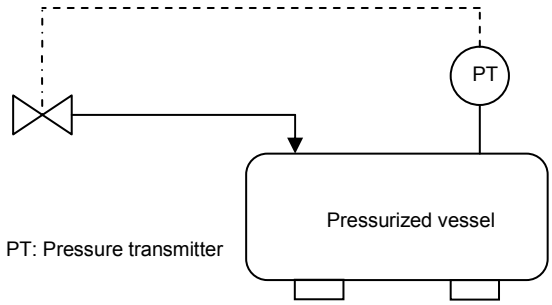

Figure 4: Process diagram of example

The safety target for the vessel is: no release to the atmosphere with an occurrence frequency greater than 10^{-4} in one year. An HAZOP (hazard and operability) analysis was performed to evaluate hazardous events that have the potential to release material in the environment. The results of the HAZOP study identify that an overpressure condition could result in a release of flammable material in the environment. A risk analysis technique indicates that the safety function required protecting against the overpressure condition needs a SIL 2. As a SIS is used to perform the safety target level for the vessel, our goal is to choose optimal SIS components and connections between them, in order to minimize the total SIS cost and obtain the SIL 2 (i.e., the reliability of SIS must be higher than 0.99). Let's consider that only 3 components type are available in the market for each subsystem. The reliability values and costs of SIS components available for each subsystem are shown in Table 2.

Tableau 2: Cost and reliability of SIS components available in the market.

SIS components	Subsystems					
	Sensors		Logic elements		Final elements	
	c_1(units)	r_1	c_2(units)	r_2	c_3(units)	r_3
Type 1	21	0.961	14	0.910	25	0.900
Type 2	15	0.930	21	0.950	35	0.940
Type 3	20	0.970	12	0.930	41	0.960

In order to find an optimal design of the SIS, a GA-based program was composed in Matlab 7.1 and executed on Pentium IV 1.3G processor. Based on the general rules presented in the the last section, we adjusted the parameters of the GA by experiments, and finally selected the following combination of the parameters:

- Size of the population: 100;
- Crossover probability: 0.60;
- Mutation probability: 0.03;
- Number of generations: 300.

The GA was executed 100 times and some statistics out of the 100 results of SIS optimal cost and reliability are given in Table 3.

Tableau 3: Statistics of optimal SIS cost, reliability and SIL over 100 runs.

Statistics	C(x)	R(x)	SIL
Average	186.4333	0.996039	2
Maximum	204	0.998104	2
Minimum	163	0.991565	2
Standard deviation	14.49062	0.001376	-

The best result for the SIS cost is 163 units, and the corresponding reliability value is 0.99092 which corresponds to SIL 1. Figure 5 represents the optimal SIS configuration obtained. The mean value of SIS cost out of the 100 solutions is 170 and the standard deviation is 6. The cost deviation indicates that the solutions found are satisfactory. The GA converges rapidly. For each run of the GA, reliability constraint was always respected ($0.99092 \le R(x) \le 0.99668$), which guaranteed the SIL 2 required for the SIS. The average execution time is about 5 s per GA run, which is very efficient.

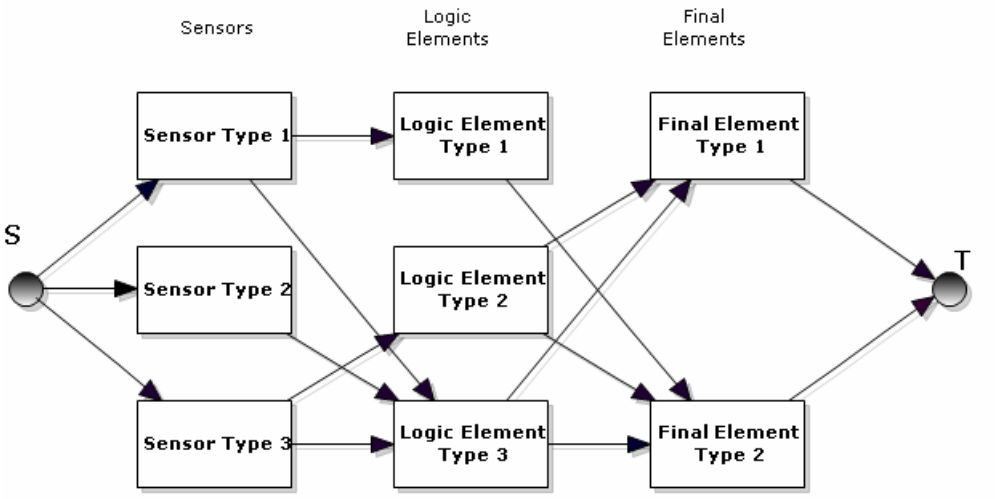

Figure 5: The optimal SIS configuration obtained (SIL 2, Cost=163)

6 – Conclusion

In this paper, we formulated an optimal design of Safety Instrumented Systems (SIS) in order to achieve the required Safety Integrity Level (SIL). The proposed method was based on the optimal choice of SIS components using a reliability graph method and a genetic algorithm.

Results from tests with several SIS components available in the market show that the proposed method is robust, with moderate computer requirements, and produce solutions satisfying the imposed constraints and presenting a considerable improvement in the SIS conception. Further research should be concentrated in taking into account failure dependencies, failure modes and periodic inspection in the optimal design of SIS.

References:

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

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

[Kuo & Prasad 00] W. Kuo, V.R. Prasad. *Reliability optimization of coherent systems*. IEEE Transactions on Reliability, 49:323-330, 2000.

[Misra 86] K. Misra. *On optimal reliability design: a review*. International Journal of Systems Science, 12:5-30, 1986.

[Coit & Smith 96] D.W. Coit, and A.E. Smith. *Solving the redundancy allocation problem using a combined neural network/genetic algorithm approch*. Computers & Operations Research, 23:515-526, 1996.

[Kuo et al. 01] W. Kuo, V.R. Prasad, F.A. Tillman, and C.L. Hwang. *Optimal reliability design: fundamentals and applications*. Cambridge, University Press, 2001.

[Yalaoui et al. 05] 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, 54:254-261, 2005.

[Sahner et al. 96] R.A. Sahner, K.S. Travedi, and A. Puliafito. *Performance and reliability analysis of computer system*. Kluwer Academic Publishers, 1996.

[Kaufmann et al. 77] A. Kaufmann, D. Grouchko, and C. Cruon. *Mathematical models for the study of the reliability of systems*. New York: Academic Press, 1977.

[Misra 70] K.B. Misra. *An algorithm for the reliability of redundant networks*. IEEE Transactions on Reliability, 19:146-151, 1970.

[Satyanarayana & Chang 83] A. Satyanarayana, and M.K. Chang. *Network reliability and the factoring theorem.* Networks, 13:107-120, 1983.

[Kim et al. 72] Y.H. Kim, K.E. Case, and P.M. Ghare. *A method for computing complex system reliability*. IEEE Transactions on Reliability, 21:215-219, 1972.

[Rai et al. 95] S. Rai, M. Veeraraghavan, and K.S. Trivedi. *A suvey of efficient reliability computation using disjoint products approach.* Networks, 25:147-163, 1995.

[Veeraraghavan & Trivedi 91] M. Veeraraghavan, and K.S. Trivedi. *An improved algorithm for symbolic reliability analysis.* IEEE Transactions on Reliability, 40:347-358, 1991.

[Holland 75] J.H. Holland. *Adaptation in natural and artificial systems*. MI: University of Michigan Press, 1975.

[Goldberg 89] D.E. Goldberg. *Genetic algorithms in search, optimization, and machine learning.* Addison Wesley, Reading, MA, 1989.

[Kumar et al. 95] A. Kumar, R.M. Pathak, Y.P. Gupta, and H.R. Parsaei. *A genetic algorithm for distributed systems topology design.* Computers and Industrial Engineering, 28:659-670, 1995.

[Painton & Campbell 95] L. Painton, and J. Campbell. *Genetic Algorithms in optimization of system reliability*. IEEE Transactions on Reliability, 44:172-178, 1995.

[Costa et al. 05] C.B.B. Costa, M.R.W. Maciel, and R.M. Filho. *Factorial design technique applied to genetic algorithm parameters in a batch cooling crystallization optimisation*. Computers & Chemical engineering, 22:2229-2241, 2005.

[ISATR] ISA-TR84.00.02-2002. *Safety Instrumented Fonctions (SIF), Safety Integrity Level (SIL), Evaluation Techniques*. Instrumentation Society of America (ISA), 2002.