# A Reliability graph approach for availability and redundancy allocation: Application to Safety Instrumented Systems

Mohamed Sallak, Christophe Simon, and Jean-Francois Aubry

CRAN UMR 7039-INPL-ENSEM,

2, Avenue de la Foret de Haye

54506, Vandoeuvre-Les-Nancy, France

mohamed.sallak@ensem.inpl-nancy.fr

jean-francois.aubry@isi.u-nancy.fr

christophe.simon@esstin.uhp-nancy.fr

## Key Words

availability; redundancy; allocation; reliability graphs; Safety Instrumented Systems (SIS); Safety Integrity Levels (SIL), safety standards.

## Summary and Conclusions

In this paper it is presented an availability and redundancy allocation method based on the use of reliability graphs. This method is not restricted to series-parallel and parallel-series systems. Furthermore, very few studies have analyzed the allocation of availability and redundancy of system components with components choice and cost constraints. An application from the technical report ISA-TR84.00.02-2002 illustrates the proposed approach in order to achieve the Safety Integrity Levels (SIL) required for Safety Instrumented Systems (SIS) under cost and components choice constraints.

## I. Introduction

IN most of the studies on reliability and redundancy allocation [1]–[4], the reliability of components may be any real between 0 and 1. In practice, there are only a fixed number of different components available in the market, which may be used in systems. There are few works which have considered this assumption. Coit and Smith [5] presented an optimization approach using a genetic algorithm (GA) and a neural network to identify the choice of components and design configuration in a series-parallel systems with a lower bound on system reliability. Kuo and Prasad [2] presented a search method (*PK-Alg*) based on lexicographic order and an upper bound on the system reliability to maximize the reliability of a coherent system over component choices and redundancy options. Yalaoui *et al.* [6] proposed a pseudopolynomial 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 took into account the market constraints.

On the other hand, there are very few works about availability and redundancy allocation. Levitin *et al.* [7] have proposed an optimal allocation based on minimizing system cost and considering failure and reparation rates by modifying components replacement frequency and preventive and corrective maintenance policies. Elegbede *et al.* [8] have developed an availability optimization of series-parallel systems based on genetic algorithms and experience plants. Castro *et al.* [9] have proposed an availability allocation based on maintenance policies of series-parallel systems. Since very few studies have analyzed the optimal design of coherent systems with components choice constraints based on availability and redundancy allocation, this paper presents an original approach using reliability graphs. This approach is not restricted to series-parallel and parallel-series systems.

Furthermore, we propose the use of this approach for the optimal design of safety systems. Today, The process industry tends to be technically complex and has the potential to inflict serious harm to people and property if the trip cannot avoid harm or during a spurious trip (*i.e.* the safety function is carried out without a demand from the process). In spite of the application of a wide variety of safeguarding measures, many accidents still happen. Experiences gained from these accidents have led to the application of a variety of technical and non-technical layers of protection, such as Safety Instrumented Systems (SIS). The SIS consists of instrumentation or controls that are implemented for the purpose of mitigating a risk or bringing the process to a safe state in the case of a process failure. Risk in process industry is defined as a measure of human injury, environmental damage or economic loss in terms of both the incident likelihood and the magnitude of the injury, damage, or loss. A SIS is used for any process in which a process hazards analysis (PHA) has determined that the mechanical integrity of the process equipment, the process control, and other protective equipments are insufficient to mitigate the potential risk. The IEC

61508 [10] and IEC 61511 [11] 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. 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. Therefore, allocation methods are necessary to determine availability and redundancy allocation in SIS, in order to minimize the SIS cost fulfilling the constraints of SIL and cost.

This paper is organized as follows. Section 2 presents definitions and basic concepts of reliability graphs. A genetic algorithm is developed to solve the allocation problem in section 3. Section 4 presents an application from the literature [12] to design a SIS with SIL and cost constraints. The SIS configurations for each SIL required are presented. Some concluding remarks and conclusions are given in section 5. Finally, section 6 presents our future works.

## II. Reliability graphs

### A. *Definitions and basic concepts*

A very efficient method to compute the availability of a system is to express it as a reliability graph [13]–[18]. Reliability graph consists of a set of arcs and nodes. The arcs represent the system elements. The nodes of the graph tie the arcs together and form the structure. The reliability graph contains one source node *O* with no incoming arcs and one sink node *Z*, with no outgoing arcs, also called destination or termination. Fig. 1 shows the reliability graph of a bridge system. The arcs represent the system components *e1*, *e2*, *e3*, *e4* and *e5*. The nodes $\{$*node 1*, *node 2*, *node 3*, *node 4*$\}$ represent the connections between the system components. A system represented by a reliability graph fails when there is no path from the source *O* to the sink *Z*.

A path is defined as a set of arcs such as if these arcs are all up, the system is up. A path is minimal if it has no proper subpaths. In the example on Fig. 1, the list of minimal paths is:

$$H1 = \{e1, e4\}$$

$$H2 = \{e2, e3, e4\}$$

$$H3 = \{e2, e5\}$$

A cut is defined as a set of arcs such as if these arcs are all down, the system is down. A cut is minimal

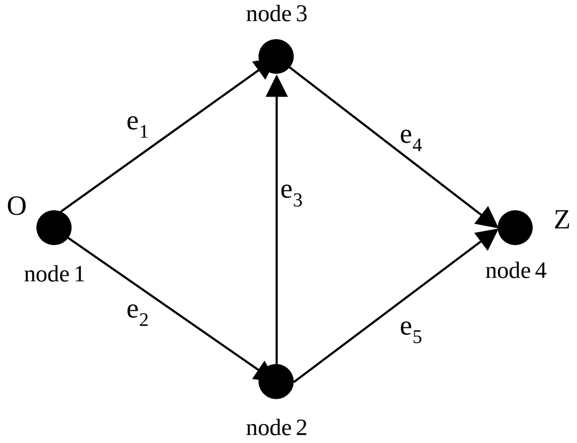

Fig. 1. Reliability graph of a bridge system

if it has no proper subcuts. In the example on Fig. 1, the list of minimal cuts is:

$$C1 = \{e1, e2\}$$

$$C2 = \{e2, e4\}$$

$$C3 = \{e4, e5\}$$

$$C4 = \{e1, e3, e5\}$$

$$C5 = \{e2, e3, e5\}$$

### *B. Reliability graph analysis*

Two classes of methods are used for reliability graph analysis. The first class of methods is minimal paths-minimal cuts enumeration. The inclusion-exclusion [15], [18], [19] or the sum of disjoint products (SDP) [20]–[23] techniques are applied to obtain the system reliability expression. The second class is the factoring methods [17], [18], [23].

*1) Minimal paths - Minimal cuts enumeration:*

*Inclusion-exclusion formula:* A method to evaluate the availability of the system is to use the Poincare's theorem, also called the inclusion-exclusion method [15], [18], [19]. Let us consider an example with only two minimal paths *H1* and *H2*. If *P(Hi)* denotes the probability that all components of minimal path Hi are operational, then, the availability of the system (*i.e.* the probability that there is a path from the source to the sink of the reliability graph) is given by:

$$A = P(H1 \cup H2) = P(H1) + P(H2) - P(H1.H2) \tag{1}$$

If the system has two minimal cuts C1 and C2, the availability of the system is given by:

$$A = 1 - P(C1 \cup C2) = 1 - [P(C1) + P(C2) - P(C1.C2)] \tag{2}$$

The inclusion-exclusion method is a generalization of this principal. Here is the inclusion-exclusion formula for $n$ minimal paths:

$$A = \sum_{i=1}^{n} P(Hi) - \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} P(Hi.Hj) +$$

$$\sum_{i=1}^{n-2} \sum_{j=i+1}^{n-1} \sum_{k=j+1}^{n} P(Hi.Hj.Hk) + ... + (-1)^{n+1} P(H1.H2.H3...Hn) \tag{3}$$

The complete computation of this formula suffers from the exponential blow-up of the number of product probabilities it requires. So this formula is essentially used for an approximation of the system reliability by keeping out the first terms of the sum.

*Sum of Disjoint Products (SDP):* Another method to evaluate the availability of the system consists in developping the availability expression so that each term is an event that does not include another event of the sum, *i.e.* all the terms are disjoints [19]–[22]. In this case, the availability is the sum of the disjoint products. This is done by using the following formula (if the system has $n$ minpaths):

$$A = P(H1) + P(\overline{H1}.H2) + ... + P(\overline{H1}.\overline{H2}...\overline{Hn-1}.Hn) \tag{4}$$

There are different ways to simplify the computation of this sum of disjoint products. The most popular one is Abraham method. In the case the number of arcs becomes large, the binary decision diagram (BDD) can evaluate efficiently the availability of the system because it uses less memory and consumes less time than others methods.

*2) Factoring method:* The principle of this method is to choose an edge and break down the reliability graph 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 edge. We

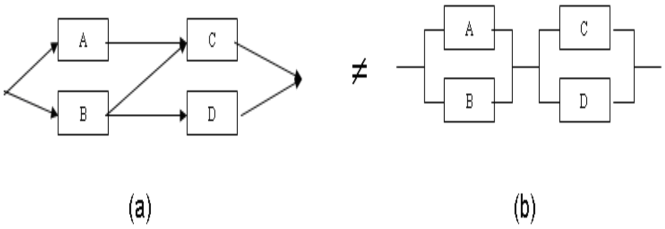

Fig. 2. Series parallel structures and reliability graphs

continue the decomposition until obtain series parallel systems which can be evaluated easily [16], [18], [23]. However, the number of factored reliability graph increases exponentially with the number of arcs.

### C. Why to use reliability graphs?

Reliability graphs can represent some complex structures which cannot be represented by series-parallel structures.

For example, the structure represented by a reliability graph in the Figure 2.a cannot be represented by a series-parallel structure. The structure in the Figure 2.b is different from the structure in the Figure 2.a. Because the structure a has 3 paths : {AC;BC;BD}. The structure b has 4 paths : {AC;BC;BD;AD}.

There are 3 main reasons to choose reliability graph in our optimal design:

- Reliability graphs can easily represent systems with complex structure.
- In the reliability graphs approach we can connect directly components between them (point to point connection).
- Once the reliability graph of the system is obtained, the corresponding adjacency matrix of the system is also formed. This matrix simplify our optimization procedure to obtain the optimal configuration of the system.

## III. Genetic algorithm implementation

### A. Introduction

Genetic algorithms (GAs) are usually used as an optimization technique with a good efficiency to search for the global optimum of a function. The GAs were developed by John Holland [24] and further described by Goldberg [25]. 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 reliability optimization problems, see e.g. [2], [18].

### B. Solution encoding

When applying GA to optimize the design of SIS, an important aspect is the encoding of the potential solutions. In our work, a potential solution (a chromosome) is a configuration of the SIS reliability graph. The encoded variables are, therefore, the arcs between reliability graph nodes. In that sense, each chromosome $x$ is coded through a vector consisting of several genes. Each gene is equal to one if there is an arc between nodes, and 0 elsewhere. Each vector $x$ corresponds to a configuration of the SIS.

### C. Reproduction

The reproduction process consists of selecting the population elements ready to reproduce by evaluating their force. This evaluation is based on the objective function. The widely used technique is the stochastic uniform selection. The algorithm lays out a line in which each parent corresponds to a section of the line of length proportional to its scaled value. The algorithm moves along the line in steps of equal size. At each step, the algorithm allocates a parent from the section it lands on.

### D. Crossing method

The crossing is the genetic operator that allows, starting from two individuals of a given generation, to create one or more other individuals of the following generation. One of the widely used technique is the scattered crossover. This crossing method creates a random binary vector and selects the genes where the vector is a 1 from the first parent, and the genes where the vector is a 0 from the second parent, and combines the genes to form the child.

### E. Mutation method

The purpose of the mutation is to bring diversity among genes. The mutation, contrary to the crossing, should not be too often applied because good genes in the individuals might be lost. In a general way, the mutation consists in modifying a gene of chromosome in a random way.

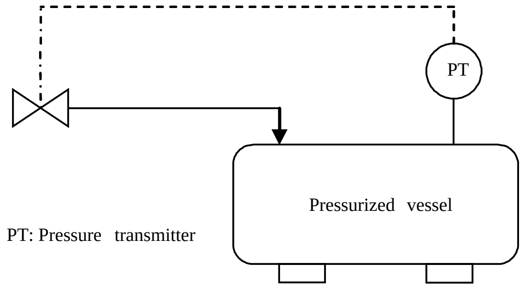

Fig. 3. Process diagram of the example [12].

### F. GA parameters

The choice of parameters for a GA can affect the performances of the algorithm. These parameters include population size, crossover rate and mutation rate. Setting GA parameters are mostly based on empirical observation with respect to the problem variety [8]. The GA parameters used in this study were retrieved from the availability design literature [26]–[28].

### G. Why to use GA?

The GA are heuristic, which means they estimate a solution. In our work, we have to estimate the average availability $A_{avg}$ and cost of SIS. These two functions are without derivatives. GA do not require this mathematical property.

## IV. Application example

To demonstrate the proposed aproach to find an optimal choice of SIS components and design configuration, we study the process defined in the technical report ISA-TR84.00.02-2002 [12].

### A. Process

The process is composed of a pressurized vessel containing volatile flammable liquid (see Figure 3). The engineered systems available are:

- An independent pressure transmitter to initiate a high pressure alarm and to alert the operator to take an appropriate action to stop inflow of material.
- In the 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.

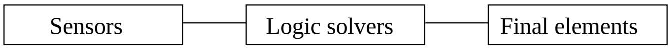

Fig. 4. A general SIS configuration

### *B. Problem description*

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 SILi ($i = 1, 2, 3$ or $4$). 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 to obtain the SILi required.

### *C. Problem formulation*

The SIS is a system composed of sensors, logic solvers and final elements for the purpose of taking the process to a safe state when predetermined conditions are violated (cf. Figure 4).

The safety performance of a SIS is defined in terms of SIL, which is defined by its $PFD_{avg}$. The $PFD_{avg}$ value is obtained from the failure probabilities of system components. This value is a function of the SIS configuration, the proof test interval, the common cause failures, and the inspection and maintenance policies. The IEC 61508 [10], IEC 61511 [11] and ISA-TR84.00.02-2002 [12] recommend several techniques to determine the $PFD_{avg}$ value. For safety functions with a low demand rate (for example anti-lock braking), and safety functions with a high demand rate or operate continuously (for example normal braking), the standards recommend values presented in Table I. In the reliability research area, the $PFD_{avg}$ of systems should be considered as an average unavailability [29], [30]. In this work, we use the SIS average availability $A_{avg}$ to determine the SIL of SIS:

$$A_{avg} = 1 - PFD_{avg} \tag{5}$$

The optimal design problem can be considered as a minimization problem of SIS cost under SIL and cost constraints. The SIL of SIS is characterized by its average availability ($A_{avg}$) over a given time period. For example, the SIL2 required means that the average availability of SIS must be higher than

TABLE I
DEFINITION OF SIL FOR LOW AND HIGH DEMAND MODES

| | Low Demand | High Demand |
|---|---|---|
| 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 | $[10^{-5}, 10^{-4}]$ | $[10^{-9}, 10^{-8}]$ |

0.99 and lower than 0.999. The cost of SIS is the sum of the cost of components in the SIS configuration. The maximum system cost allowed is $C_{max} = 20000$. Let us consider that only 3 of components type are available in the market for each subsystem. The reliability values and costs (the cost unit is euros) of SIS components available for each subsystem are given Table II. The reliability data (failure probabilities of components) and costs of components correspond to the values used in reliability database [31]–[33]. Then, the optimal design problem is to find the optimal SIS configurations (*i.e.* SIS components types and connections between the components) that:

- Minimise C(x)
- Subject to :

  $A_{min} \leq A_{avg}(x) \leq A_{max}$

  $C(x) \leq C_{max}$

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

- Size of the population: 100;
- Crossover probability: 0.90;
- Mutation probability: 0.03;
- Number of generations: 300.

## V. RESULTS AND ANALYSIS

### A. Case I: SIL 1 required

The objective is to obtain the SIL1 given the system cost constraint ($C(x) \leq C_{max}$). The maximum number of components allowed in each subsystem is 3. The GA was executed 150 times and some statistics

| SIS Components | Subsystems | | | | | |
|---|---|---|---|---|---|---|
| | Sensors | | Logic elements | | Final elements | |
| | $c_1$ | $p_1$ | $c_2$ | $p_2$ | $c_3$ | $p_3$ |
| Type 1 | 2100 | 0.039 | 1400 | 0.09 | 2500 | 0.1 |
| Type 2 | 1500 | 0.07 | 2100 | 0.05 | 3500 | 0.06 |
| Type 3 | 2000 | 0.03 | 1200 | 0.07 | 4100 | 0.04 |

TABLE II
COSTS AND FAILURE PROBABILITIES OF SIS COMPONENTS (TYPES 1, 2 AND 3)

| Statistics | C(x) | $A_{avg}(x)$ | SIL |
|---|---|---|---|
| Average | 8600 | 0.913037 | 1 |
| Maximum | 9400 | 0.927941 | 1 |
| Minimum | 8100 | 0.906056 | 1 |
| Standard deviation | 661 | 0.0092 | - |

TABLE III
STATISTICS FOR SIL1

out of the 150 results of SIS optimal cost and availability are given in Table III. The best result obtained for the SIS cost is 8100 units, and the corresponding availability value is 0.906056 which corresponds to SIL1. The mean value of SIS cost out of the 150 solutions is 8600 units and the standard deviation is 661. The cost deviation indicates that the solutions found are satisfactory. For each run of the GA, availability and cost constraints were always respected. Figures 5 and 6 show the two best obtained reliability graphs, and Figures 7 and 8 show SIS configurations obtained from these reliability graphs. In reliability graphs, the element $k_i$ denotes the sensor type $i$, the element $l_i$ denotes the logic element type $i$ and the element $m_i$ denotes the final element type $i$.

We remark that the figure 7 presents a classical series-parallel system which is composed of:

- 1 sensor (type 3)
- 2 logic elements (types 1 and 3)
- 1 final element (type 1)

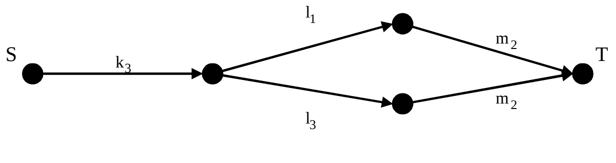

Fig. 5. Reliability graph (SIL1: $A_{avg} = 0.906056, C = 8100$)

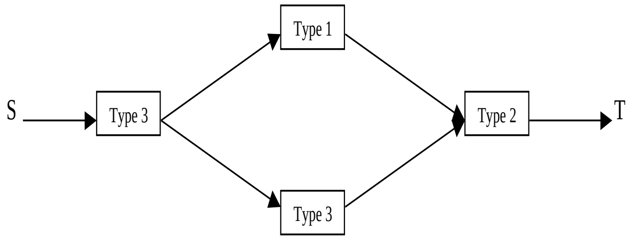

Fig. 6. SIS configuration (SIL1: $A_{avg} = 0.906056, C = 8100$)

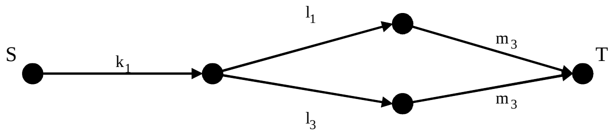

Fig. 7. Reliability graph (SIL1: $A_{avg} = 0.916748, C = 8800$)

### B. Case II: SIL 2 required

We consider the same objectives for system cost and maximum number of allowed components in each subsystem. The GA was executed 150 times. The statistics of SIS optimal cost and availability are given in Table IV. The best result obtained for the SIS cost is 13400 units, and the corresponding availability value is 0.990326 which corresponds to SIL2. The mean value of SIS cost is 15000 units and the standard deviation is 700. The cost deviation indicates that the solutions found are satisfactory. For each run of the GA, availability and cost constraints were always respected. Figures 9 and 11 show the two best obtained reliability graphs, and Figures 10 and 12 show SIS configurations obtained from these reliability graphs. The Figure 10 presents a complex structure composed of:

- 2 sensors (types 2 and 3)
- 3 logic elements (types 1,2 and 3)
- 2 final elements types 1 and 2)

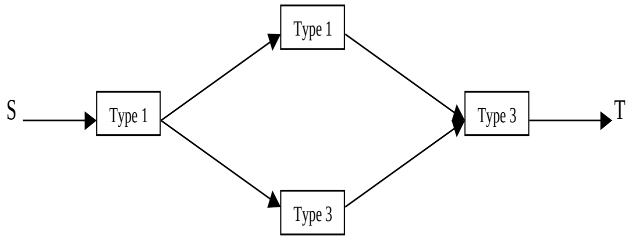

Fig. 8. SIS configuration (SIL1: $A_{avg} = 0.916748, C = 8800$)

| Statistics | C(x) | $A_{avg}(x)$ | SIL |
|---|---|---|---|
| Average | 15000 | 0.992039 | 2 |
| Maximum | 16400 | 0.995124 | 2 |
| Minimum | 13400 | 0.990326 | 2 |
| Standard deviation | 700 | 0.001176 | - |

TABLE IV
STATISTICS FOR SIL2

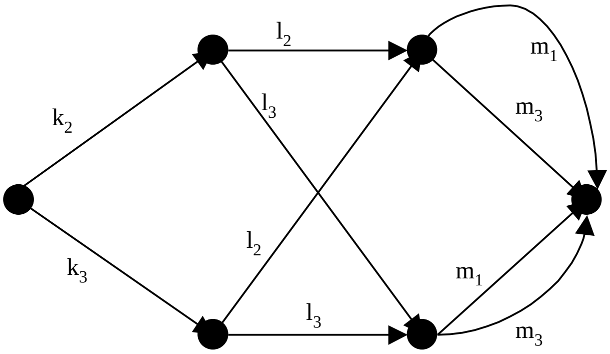

Fig. 9. Reliability graph (SIL2: $A_{avg} = 0.990430, C = 13400$)

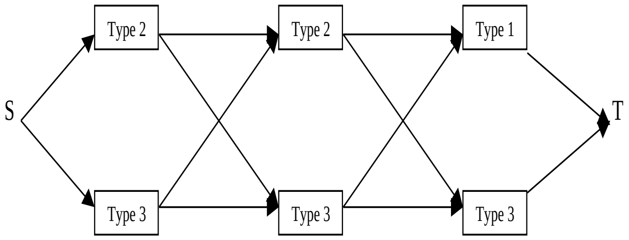

Fig. 10. SIS configuration (SIL2: $A_{avg} = 0.990326, C = 13400$)

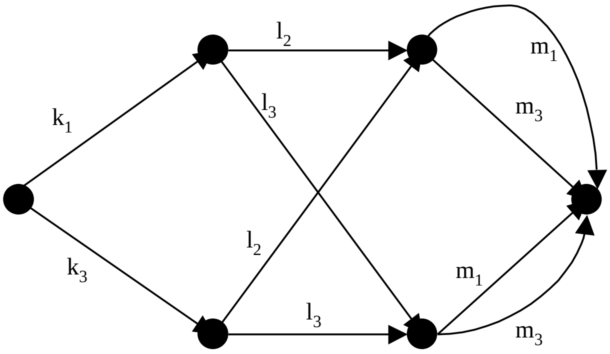

Fig. 11. Reliability graph (SIL2: $A_{avg} = 0.991353, C = 13600$)

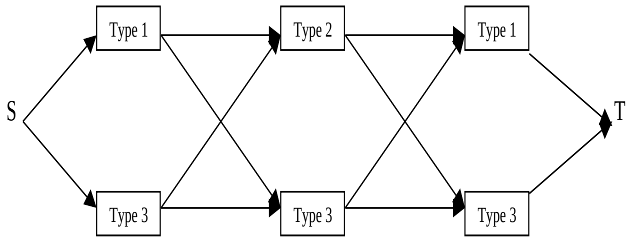

Fig. 12. SIS configuration (SIL2: $A_{avg} = 0.991353, C = 13600$)

| Statistics | C(x) | $A_{avg}(x)$ | SIL |
|---|---|---|---|
| Average | 20400 | 0.99932 | 3 |
| Maximum | 20400 | 0.9994 | 3 |
| Minimum | 20400 | 0.9993 | 3 |
| Standard deviation | 0 | 0.000121 | - |

TABLE V
STATISTICS FOR SIL3

### C. Case III: SIL 3 required

We consider the same objectives for system cost and maximum number of allowed components in each subsystem. The GA was executed 150 times. The statistics of SIS optimal cost and availability are given in Table V. The best result obtained for the SIS cost is 20400 units, and the corresponding availability value is 0.9993 which corresponds to SIL3. The mean value of SIS cost is 20400 units and the standard deviation is 0. There is no cost deviation. In each run of the GA, availability and cost constraints were always respected. Figures 13 and 15 show the two best obtained reliability graphs, and Figures 14 and 16 show SIS configurations obtained from these reliability graphs. The Figure 10 presents a complex structure composed of:

- 3 sensors (types 1, 2 and 3)
- 3 logic elements (types 1, 2 and 3)
- 3 final elements types 1, 2 and 3)

### D. Case IV: SIL4 required

We consider the same objectives for system cost and maximum number of allowed components in each subsystem. The GA was executed 150 times. We did not obtain SIS configurations which satisfy the required SIL and cost constraints. Because the reliability values of SIS components (type 1, 2 and 3 for each subsystem) are not high enough to obtained a high availability value of SIS (the SIL4 required

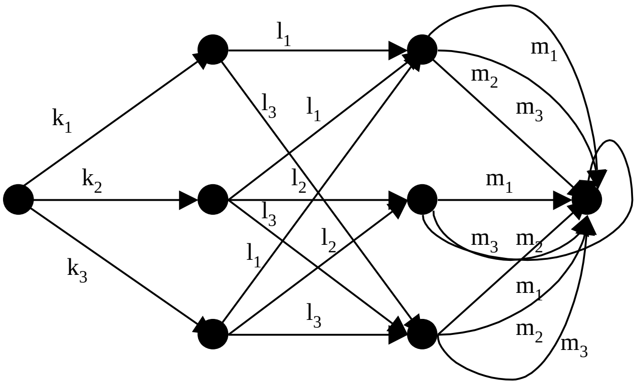

Fig. 13. Reliability graph (SIL3: $A_{avg} = 0.9993, C = 20400$)

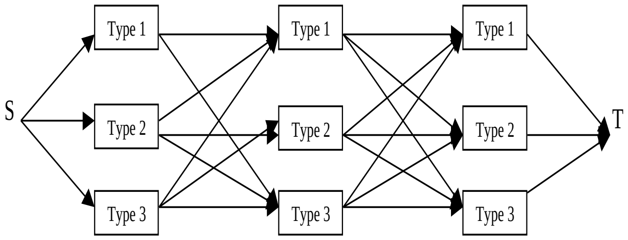

Fig. 14. SIS configuration (SIL3: $A_{avg} = 0.9993, C = 20400$)

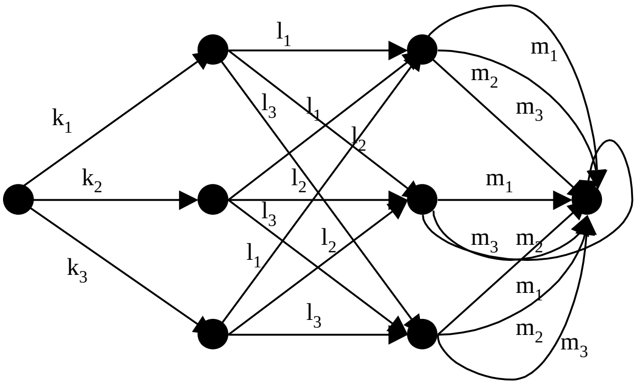

Fig. 15. Reliability graph (SIL2: $A_{avg} = 0.9994, C = 20400$)

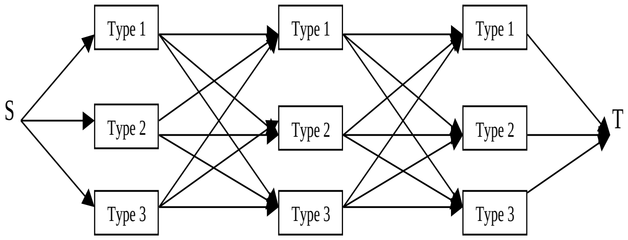

Fig. 16. SIS configuration (SIL3: $A_{avg} = 0.9994, C = 20400$)

| SIS components | Subsystems | | | | | |
|---|---|---|---|---|---|---|
| | Sensors | | Logic elements | | final elements | |
| | $c_1$ | $p_1$ | $c_2$ | $p_2$ | $c_3$ | $p_3$ |
| Type 5 | 2100 | $0.019$ | 1400 | $0.04$ | 2500 | $0.02$ |
| Type 6 | 1500 | $0.03$ | 2100 | $0.05$ | 3500 | $0.03$ |
| Type 7 | 2000 | $0.0225$ | 1200 | $0.03$ | 4100 | $0.04$ |

TABLE VI

COSTS AND FAILURE PROBABILITIES OF SIS COMPONENTS (TYPES 4, 5 AND 6)

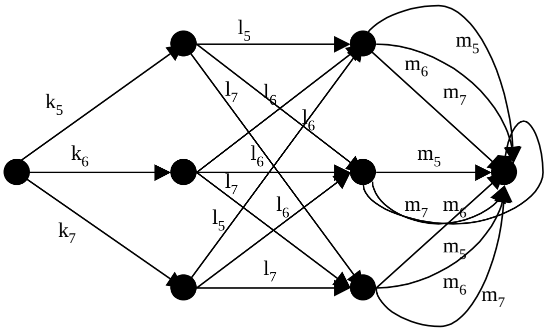

Fig. 17. Reliability graph (SIL4: $A_{avg} = 0.9999003, C = 20400$)

$A_{min} = 0.9999$. That's why we propose the use of more reliable components. The cost and reliability values of these components are presented in Table VI. The GA was also executed 150 times. In this case, we obtain the SIL4. Figure 17 shows the reliability graph obtained, and Figure 18 shows the SIS configuration obtained from this reliability graph. The SIS configuration (cf. Figure 18) is a complex structure composed of:

- 3 sensors (types 5, 6 and 7)
- 3 logic elements (types 5, 6 and 7)
- 3 final elements (types 5, 6 and 7)

We conclude that in order to obtain the SIL4, we have to use a more reliable SIS components or to modify the system constraints.

Furthermore, the SIS configurations obtained for the SIL4 required have the maximum number of connection between components (3 connections for each component) because we don't consider the connections cost, we consider only the components cost.

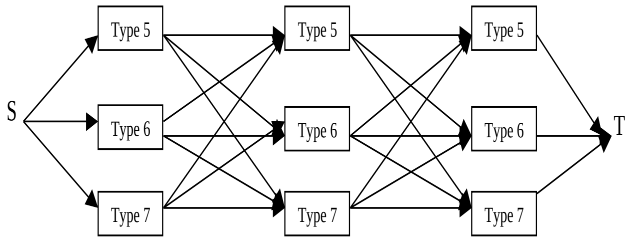

Fig. 18. SIS configuration (SIL4: $A_{avg} = 0.9999003, C = 20400$)

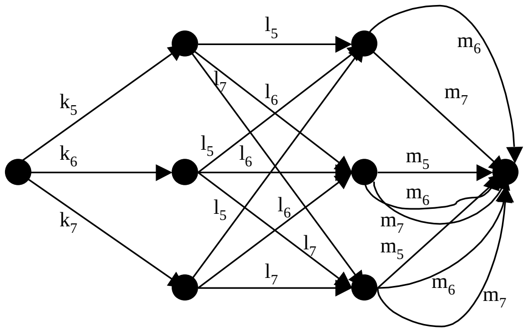

Fig. 19. Reliability graph (SIL4 with costs connections: $A_{avg} = 0.999902, C = 27600$)

### *E. Case V: Taking into account the connections cost*

We consider the SIL4 required and we add the connections cost to the SIS cost. The overall connections have the same costs (200 units). We consider the same maximum number of allowed components in each subsystem. The GA was executed 150 times. We remark that the best obtained SIS configuration (cf. Figures 19 and 20) which have 23 connections is different from the best configuration obtained when we don't take into account the connections cost (cf. Figures 17 and 18) which have 24 connections. We conclude that we don't obtain the same optimal configurations if the cost connections is added to the SIS cost.

On the other hand, we have to consider the reliability of connections. In the most cases, the reliability researchers consider that the reliability of connections are included in the reliability of components. Furthermore, instead of connections we can use bus communication which reduce the cost of system design. But in this case, we have to take into account the study of the bus reliability in the optimal design methodology.

## VI. Conclusion

In this paper, we formulated an original approach based on reliability graph for availability and redundancy allocation. This approach was used for the optimal design of Safety Instrumented Systems

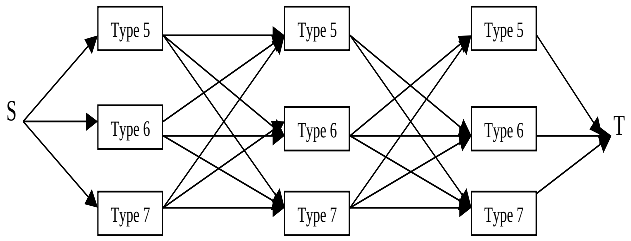

Fig. 20. SIS configuration (SIL4 with cost connections: $A_{avg} = 0.999902, C = 27600$)

(SIS) in order to achieve the required Safety Integrity Level (SIL). The proposed method was based on the optimal choice of components and the connections between them, and it is not restricted to series-parallel and parallel-series systems.

Results from tests with several SIS components available in the market show that the proposed method produce solutions satisfying the constraints and presenting a considerable improvement in the SIS conception.

Further research should be concentrated in taking into account reliability of connections, failure dependencies, failure modes and periodic inspections.

## REFERENCES

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

[2] W. Kuo and V. Prasad, “Reliability optimization of coherent systems,” *IEEE Transactions on Reliability*, vol. 49, pp. 323–330, 2000.

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

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

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

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

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

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

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

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

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

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

[13] R. Sahner, K. Trivedi, and A. Puliafito, *Performance and Reliability Analysis of Computer System*. Kluwer Academic Publishers, 1996.

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

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

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

[17] R. Wood, "A factoring algorithm using polygontochain reductions for computing k-terminal network reliability," *Networks*, vol. 15, pp. 173–190, 1985.

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

[19] P. Lin, B. Leon, and T. Huang, "A new algorithm for symbolic system reliability analysis," *IEEE Transactions on Reliability*, vol. 25, pp. 2–15, 1976.

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

[21] T. Luo and K. Trivedi, "An improved algorithm for coherent system reliability," *IEEE Transactions on Reliability*, vol. 47, pp. 73–78, 1998.

[22] S. Rai, M. Veeraraghavan, and K. Trivedi, "A survey of efficient reliability computation using disjoint products approach," *IEEE Networks*, vol. 25, pp. 147–163, 1995.

[23] S. Soh and S. Rai, "Computer aided reliability evaluator for distributed computing networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 2, pp. 199–213, 1999.

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

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

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

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

[28] T. Yokota, M. Gen, and Y.-X. Li, "Genetic algorithm for non-linear mixed integer programming problems and its applications," *Computers and Industrial Engineering*, vol. 30, pp. 905–917, 1996.

[29] F. Innal, Y. Dutuit, and M. Djebabra, "An analysis of simplified equations in cei 61508-6," in *Proceedings of the QUALITA 2005 Conference, Bordeaux, France*, 2005.

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

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

[32] *Safety Equipment Reliability Handbook, 2nd Edition*. Exida, 2005.

[33] S. Hauge, H. Langseth, and T. Onshus, *Reliability Data for Safety Instrumented Systems, PDS Data Handbook*. Sintef, 2006.

**Jean-Francois Aubry** is a full professor at the Ecole Nationale Superieure d'Electricite et de Mecanique, an engineers high school of the Institut National Polytechnique de Lorraine, in France where he is in charge of Discrete Event Systems and Reliability, Availability, Maintainability, and Safety courses. He is a research director at the Research Centre for Automatic Control (CRAN), a CNRS labeled laboratory and works especially on the design and dependability assessment of automatic control systems and particularly safety instrumented systems. Since 1998, he is the head of the ”Institut de Surete Industrielle” (a federative institute of the four Universities in Lorraine) for research and training in the field of quality, safety, dependability and environmental impact of industrial activity.

**Christophe Simon** received the M.S. degree in Metrology, Control Systems and Electrotechnic in 1991 and the Ph.D. degree in 1996. In 1999, he joined the Department of Quality, Industrial Logistic and Organization of the IUT of Epinal as an assistant professor. He is head of the department since 2004. He has joined the Research Centre for Automatic Control in 1992 and his research area concern reliability and systems safety, pattern recognition, fuzzy logic, possibility theory and evidence theory. He is a member of French Association of Electrical, Electronic and System Control Association (Club EEA).

**Mohamed Sallak** received the M.S. degree from the Ecole Nationale Superieure d'Electricite et de Mecanique, an engineers high school of the Institut National Polytechnique de Lorraine, in France, in 2003 and and the Ph.D. degree in 2007. He is currently working in the field of design and dependability assessment of automatic control systems with the Research Centre for Automatic Control, in France. His research interests include applying fuzzy set theory to evaluate reliability of safety related systems under uncertainty and optimal design of Safety Instrumented systems.