Optimal Design of Safety Instrumented Systems

Mohamed Sallak, Christophe Simon, Jean-François Aubry

OPTIMAL DESIGN OF SAFETY INSTRUMENTED SYSTEMS

Mohamed Sallak, Christophe Simon, and Jean-François Aubry

Centre de Recherche en Automatique de Nancy (CRAN) / UMR 7039,
Nancy-university, CNRS, France.
ENSEM, 2 Avenue de la forêt de Haye,
54506 Vandoeuvre-Les-Nancy.
mohamed.sallak@ensem.inpl-nancy.fr
christophe.simon@esstin.uhp-nancy.fr
jean-françois.aubry@isi.u-nancy.fr

Abstract: This paper presents an optimization model of availability and redundancy allocation of Safety Instrumented Systems (SIS) in order to achieve the required Safety Integrity Level (SIL). The SIL level is addressed by ANSI/ISA S84.01-1996 and IEC 61508 safety standards. The optimal allocation is based on the use of genetic algorithms. An example which illustrates the use of the optimization model to achieve a SIL level 1 under budget and components choice constraints is proposed.

Keywords: Safety Instrumented Systems, Safety Integrity Levels, Optimization, Availability, Redundancy, Genetic algorithms.

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 protection layers, such as Safety Instrumented Systems (SIS). The SIS consists in 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. A SIS is used for any process in which a process hazards analysis (PHA) has determined that the integrity of the process equipment, the process control, and other protective equipments are insufficient to mitigate the potential risk. The ANSI/ISA S84.01-1996 (ISA, 1996) and IEC 61508 (IEC, 1998) safety standards provide guidelines for the design, installation, operation, maintenance and test of SIS.

However, in the field there is a considerable lack of understanding how to apply these standards in order to design SIS to meet the required SIL. The use of redundant components increases the SIL level, but it also increases design and maintenance costs. Therefore, optimization methods are necessary to determine how many redundancies, and availability parameters must be used in each component or subsystem, in order to maximize the SIL level fullfilling constraints of cost.

Several papers related to systems reliability optimization using genetic algorithms was published in the last few years such as Tilleman et al. (1977), Tzafestas et al. (1980), Dhillon (1980), Misra (1986), Painton et al. (1995), Coit and Smith (1996), Yang et al. (1999), Kuo et al. (2001), Vidyarthi and Tripathi (2001), and Yalaoui et al. (2005).

In contrast to reliability optimization, fewer researchers have studied availability optimization to find out the optimal failure and repair rates for each component in a system for maximizing or minimizing the objectives. Levitin and Lisnianski (1999) proposed an optimization procedure that minimizes the total system cost, considering failure and repair time. Castro and Cavalca (2003) developed an availability optimization, with redundancy allocation and team maintenance action as parameters. Elegbede and Adjallah (2003) proposed a methodology based on genetic algorithms and experiment plans to optimize the availability and the cost of reparable systems.

The aim of this paper is to present a procedure of availability and redundancy allocation of Safety Instrumented Systems (SIS) in order to achieve the required Safety Integrity Level (SIL). The procedure is based on the use of genetic algorithms. An example from the literature (ISA-TR84.00.02, 2002) which illustrates the use of the optimization model to achieve a SIL level 1 under cost and components choice constraints is proposed.

2. PROCEDURE TO ACHIEVE THE SAFETY TARGET LEVEL OF THE PROCESS

This section focuses on quantitative techniques that can be used to evaluate the risk associated to a process. After the risk has been evaluated, we have to identify the necessary Safety Instrumented Functions (SIF) to be implemented on a SIS in order to achieve the desired SIL. All these steps are required in order to comply with the ANSI/ISA S84.01-1996 (ISA, 1996) and IEC 61508 (IEC, 1998) safety standards.

2.1 Safety Instrumented Systems (SIS)

The SIS is a system composed of sensors, logic solver and final elements for the purpose of taking the process to a safe state when predetermined conditions are violated. The safety performance of the SIS is defined in terms of SIL, which is defined by the average availability A_{avg}. The ANSI/ISA S84.01-1996 (ISA, 1996) and IEC 61508 (IEC, 1998) recommend techniques to determine the A_{avg} value. For safety functions with a low demand rate (for example the anti-lock braking in a car), and safety functions with a high demand rate (for example the normal braking in a car), the standards use Table 1.

Table 1. Definition of SIL for low and High Demand modes

Solicitation	**Low Demand**	**High Demand**
SIL	A_{avg}	Failures/hour
4	[0.9999;0.99999]	$[10^{-9};10^{-8}]$
3	[0.999;0.9999]	$[10^{-8};10^{-7}]$
2	[0.99;0.999]	$[10^{-7};10^{-6}]$
1	[0.90;99]	$[10^{-6};10^{-5}]$

2.2 Compliance with ANSI/ISA S84.01-1996 and IEC 61508 standards

The basic steps required to comply with the ANSI/ISA S84.01-1996 (ISA, 1996) and IEC 61508 (IEC, 1998) safety standars are the following:

- Identify the safety target level of the process.
- Evaluate the hazardous events that pose a risk higher than the safety target level.
- Determine the safety functions that must be implemented on a SIS to achieve the safety target level.
- Implement the safety functions on a SIS and evaluate its SIL.
- Install, test and commission the SIS.
- Verify that the installed SIS does reduce the process risk to below the safety target level.

3. AVAILIBILITY AND COST MODELS

3.1 Notations

C_s	Total system cost
A_{avg}	System average availability
λ_i	Failure rate of component *i*
μ_i	Repair rate of component *i*
k_i	Number of components in subsystem *i.*

3.2 Assumptions

- All systems consist of s-independent components/subsystems.
- The system and its components/subsystems can only assume two states, failed and operational.
- The system structure is coherent.
- In repairable systems, only the failure and repair rates of the components/subsystems are considered.

3.3 Availability model

Reliability and availability are both measures of the system performance. System reliability evaluates the surviving opportunity of the system for a given period of time, whereas system availability stands for the online level of the system. For repairable systems, availability is a more meaningful measure than reliability to measure the effectiveness of maintained systems, because it includes reliability as well as maintainability.

Availability can be calculated by the ratio between the mean time between failure (MTBF) and the mean time to repair (MTTR):

$$A = \frac{MTBF}{MTBF + MTTR} \qquad (1)$$

In availability analysis, an exponential distribution is initially assumed to be representative for the reliability and maintainability statistical models. The MTBF is the inverse of the failure rate:

$$MTBF = \frac{1}{\lambda} \qquad (2)$$

Similarly, the MTTR is the inverse of the repair rate:

$$MTTR = \frac{1}{\mu} \qquad (3)$$

Then, the average availability A_{avg} can be expressed by the equation below:

$$A_{avg} = \frac{\mu}{\mu + \lambda} \qquad (4)$$

For the parallel-series systems (see Fig. 1), if we suppose that in each subsystem *i*, all components have the same failure rate λ_i and the same repair rate μ_i, the average system availability is given by:

$$A_{avg} = \prod_{i=1}^{s} \left(1 - \left(\frac{\lambda_i}{\lambda_i + \mu_i} \right)^{k_i} \right) \qquad (5)$$

Where k_i is the number of components in each subsystem i, s is the number of subsystems.

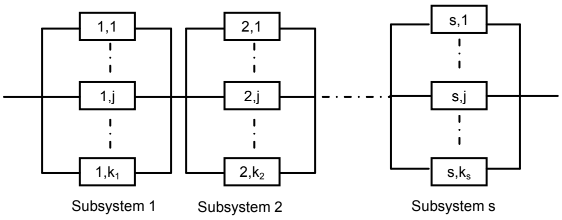

Fig. 1. General structure of parallel-series system.

3.4 Cost model

One can hardly perceive obtaining the SIL required without including cost consideration. In this paper, we use the cost function defined by Elegbede and Adjallah (2003), because it takes into account both failure and repair rate:

$$C_S = \sum_{i=1}^{S} k_i \left(a_i \lambda_i^{p_i} + b_i \mu_i^{q_i} \right) \qquad (6)$$

Where a_i, b_i and q_i are positive real numbers, while p_i is negative (i=1, 2, …, s). These coefficients are often obtained from a maintenance data base.

4. A GENETIC ALGORITHM TO OPTIMIZE SIL AND COST

4.1 Introduction

Traditional methods, such as the Lagrange Multiplier (Ramakumar, 1993), are inefficient with problems involving large number of parameters, because they demand complex mathematics, making computational implementation difficult and lacking in flexibility. Besides, some search methods can converge only to local optima. The genetic algorithms (Goldberg, 1989) are a search method based on concepts of biological evolution and reproduction. Previous works (Goldberg, 1989) indicate that genetic algorithms are recommended for problems involving complex mathematical expressions in their modeling. An important advantage is that they do not require the use of differential calculus.

The genetic algorithms were developed by John Holland in 1967 (Davis, 1991; Goldberg, 1989) at the Michigan University. The implementation of the genetic algorithms consists in creating an initial population with given size (number of individuals). Then by a selection process similar to that of the natural selection, which is defined by an adaptation function, the second step is to select the individuals who will be crossed. These individuals are represented by a chromosome in the genetic algorithm. Then a current population is created by crossing of the individuals. The passage from a current population to another is called generation. For each generation, the algorithm keeps the individual with the best criterion value. The coding and the construction of the chromosome, representing the individual in the population, is the most important step of the algorithm. The general structure of the genetic algorithm is as follows.

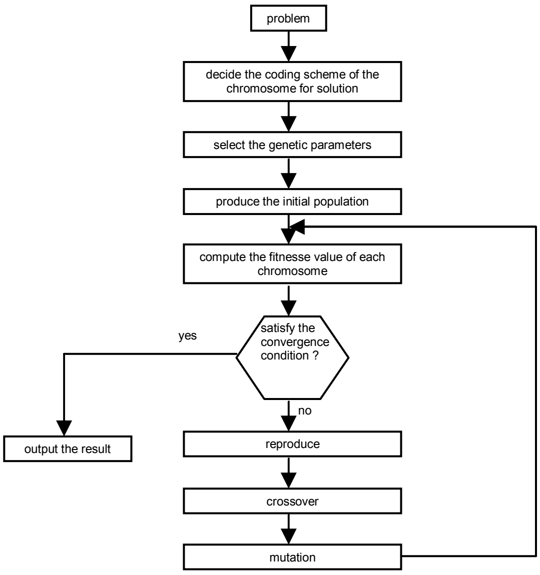
problem
decide the coding scheme of the chromosome for solution
select the genetic parameters
produce the initial population
compute the fitnesse value of each chromosome
satisfy the convergence condition ?
yes
no
output the result
reproduce
crossover
mutation

Fig. 2. A simple genetic algorithm framework.

To resolve the availability and redundancy allocation, we use a genetic algorithm. The optimal decision variables to be determined are the number of components k_i, the failure rate λ_i and the repair rate μ_i of each component for the i^{th} subsystem. We suppose that failure and repair rates of SIS components are constants.

4.2 Parameters encoding

The decision variables of an optimization problem can be represented as an artificial chromosome consisting of numerous artificial genes. Several genes are used to express a decision variable. This paper uses the string encoded genes, since the encoding is easy and there is high precision in representing a parameter. We express the decision variables in a chromosome as:

$$\left[\lambda_1 \quad \lambda_2 \ldots \quad \lambda_m \quad \mu_1 \quad \mu_2 \ldots \quad \mu_m \quad k_1 \quad k_2 \ldots \quad k_m \right]$$

The initial population is generated randomly based on the encoding of chromosomes.

4.3 Reproduction

The reproduction process consists of selecting the population elements ready to reproduce by evaluating their force, i.e. the ready ones are the strongest. This evaluation is based on the adaptation function which is the objective function in the case of maximization without constraint. In this paper, we have to assure the feasibility of the solution before calculating the objective function. From a generation to another we sort all the individuals, in the intermediate generation, and choose the N best ones.

4.4 The 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. We choose randomly to be crossed, with a probability of P_c=0.5 (Grefenstette, 1986), *N/2* couples of individuals. Among the variety of crossover operators, we adopt those produce from each crossing two children. This operator is generally called *1X* (Goldberg, 1989). This crossover operator consists of generating randomly a point, called crossover point, and combines the different parts of the parent chromosomes to construct the children ones.

4.5 The 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. The mutation probability adopted is P_m=0.03 (Grefenstette, 1986). It consists in modifying a part of chromosome in a random way. This modification consists in permuting between two genes chosen randomly for each selected chromosome.

4.6 The population size and the generation number

The size of the population was fixed at *N*=200. It appears that, if this size is too low, there will be risk to obtain not enough varied solutions by the individual crossing (Grefenstette, 1986). Performing many control tests, we decided finally to fix the value to 150.

5. APPLICATION EXAMPLE

In order to illustrate the approach proposed in this paper, let us consider a process composed of a pressurized vessel containing volatile flammable liquid (see Fig. 3). 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.

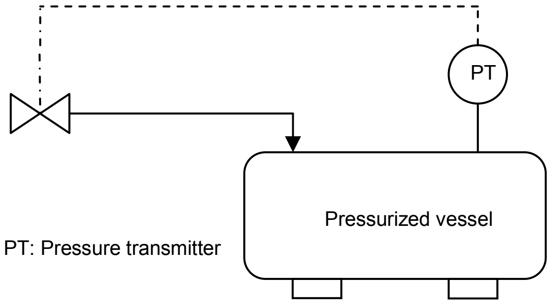

Fig. 3. Process diagram of example.

The safety target for the vessel is: no release to the atmosphere with a frequency of occurrence 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, and a risk analysis technique indicates that the safety function required protecting against the overpressure condition needs a SIL 1. As a SIS is used to perform the safety target level for the vessel, our goal is to maximize A_{avg} and minimize C_s in order to obtain the SIL 1. The example process and the SIS are defined in ISA-TR84.00.02 (2002) (see Fig. 4).

We use parallel serie system to describe the SIS as illustrated in Fig. 3. The system structure is composed of three subsystems:

- Subsystem sensors (S);
- Subsystem logic elements (LE);
- Subsystem final elements (FE).

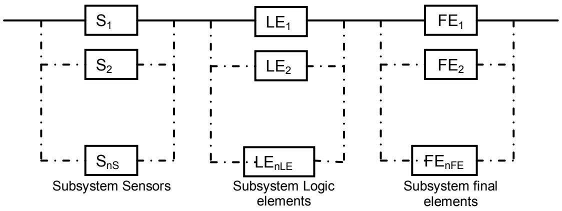

Fig. 4. Safety Instrumented System.

Without loss of generality, suppose that all components are identical (ie. SIS components have the same failure and repair rates) in each subsystem. According to Table 1, SIL 1 means that:

$$0.90 \le A_{avg} \le 0.99$$

We have two objectives, i.e. maximizing SIL level (system availability A_{avg}) and minimizing system cost C_S subject to: (6)

$$A_{avg\min} \le A_{avg} \le A_{avg\max}$$

$$C_S \le C_{\max}$$

$$n_{S\min} \le n_S \le n_{S\max}$$

$$n_{LE\min} \le n_{LE} \le n_{LE\max}$$

$$n_{FE\min} \le n_{FE} \le n_{FE\max}$$

$$\lambda_{Si\min} \le \lambda_{Si} \le \lambda_{Si\max}$$

$$\mu_{Si\min} \le \mu_{Si} \le \mu_{Si\max}$$

$$\lambda_{LEi\min} \le \lambda_{LEi} \le \lambda_{LEi\max}$$

$$\mu_{LEi\min} \le \mu_{LEi} \le \mu_{LEi\max}$$

$$\lambda_{FEi\min} \le \lambda_{FEi} \le \lambda_{FEi\max}$$

$$\mu_{FEi\min} \le \mu_{FEi} \le \mu_{FEi\max}$$

Where $n_{Subsystem\_i}$ represents the number of components in susbsystem *i*.

The lower and upper values for failure and repair rates of SIS components, the target SIS availability (target SIL), and cost are provided in Table 2. Furthermore, we have provided the number of allowed components in each subsystem. We apply the optimization method previousely defined to the SIL and cost allocation problem.

Table 2. Upper and lower values for variable decisions

Decision variables	Lower value	Upper value
A_{avg}	0.90	0.99
n_S	2	10
n_{LE}	2	5
n_{FE}	2	10
λ_{Si}	$8.6\ 10^{-4}$	$9.4\ 10^{-3}$
λ_{LEi}	9.10^{-4}	9.10^{-3}
λ_{FEi}	8.10^{-4}	8.10^{-3}
μ_{Si}	10^{-3}	8.10^{-3}
μ_{LEi}	10^{-3}	10^{-2}
μ_{FEi}	10^{-3}	8.10^{-3}
C_S	-	110

At the 115th generation of the chromosome and goal function variables, the fitness value (objective function) does not change (see Fig. 5). In the final optimal solution (see Fig. 6), the optimal SIS availability obtained is 0.90, which corresponds to SIL 1 and respect the SIL target. The optimal SIS cost obtained is 92.85 units, which is lower than the cost upper value (110 units).

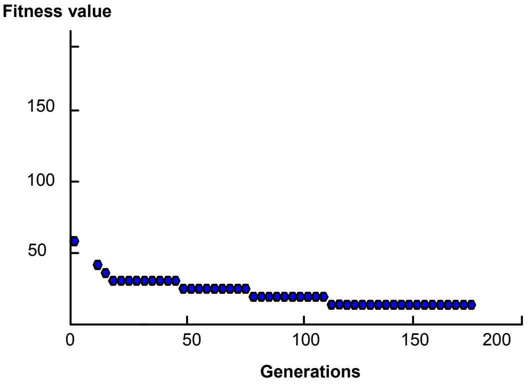

Fig. 5. Convergence results.

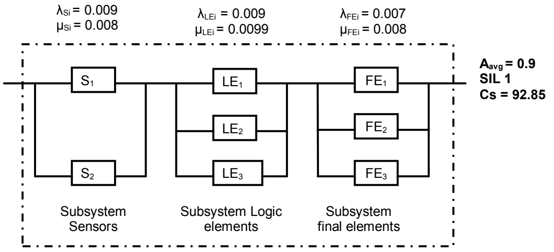

Fig. 6. Optimal SIS configuration.

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 redundancy and availability allocation of SIS components using genetic algorithms. The efficiency has been realized in numerical example from the literature (ISA-TR84.00.02, 2002). Further research should be concentrated in obtaining an optimal design of SIS which have complex structure.

REFERENCES

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

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

Coit, D.W. and A.E. Smith (1996). Reliability optimization of series-parallel systems using a genetic algorithm. *IEEE Transactions on Reliability*, **45**, pp. 254-260.

Davis, L. (1991). *Handbook of genetic algorithms.* New York: Van Nostrand Reinhold.

Dhillon, B.I. (1980). Reliability apportionment/ allocation: a survey. *Microelectronics and Reliability*, **26**, pp. 1121-1129.

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

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

Grefenstette, J. J. (1986), Optimization of control parameters for genetic algorithms. *IEEE Trans. Systems, Man, and Cybernetics,* **16**, pp. 122-128.

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

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

Kuo, W., V.R. Prasad, F.A. Tillman and C.L. Hwang (2001). *Optimal Reliability Design: Fundamentals and applications*, University Press, Cambridge.

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

Misra, K. (1986). On optimal reliability design: a review. *System Science*, **12**, pp. 5-30.

Moore, L., K. Bhimavarapu, and P. Stavrianidis. (1997). *Performance based safety standards: an integrated risk assessment program.*

Instrumentation Society of America, Technical Report.

Painton, L. and J. Campbell (1995). Genetic algorithms in optimization of system reliability. *IEEE Transactions on Reliability,* **44**, pp. 172-180.

Ramakumar, R. (1993). *Engineering reliability*. Englewood Cliffs, NJ: Prentice-Hall.

Summers, A.E. (2002). Viewpoint on ISA TR84.00.02: simplified methods and fault tree analysis. *ISA Transactions*, **39**, pp. 125-131.

Tillman, F.A., C.L. Hwang, and W. Kuo (1977). Optimization techniques for systems reliability with redundancy. *IEEE Transactions on Reliability*, **26**, pp. 148-155.

Tzafestas, S.G. (1980). Optimization of system reliability: A survey of problems and techniques. *International Journal System Science*, **11**, pp.455-486.

Vidyarthi, D.P. and A.K. Tripathi (2001). Maximizing reliability of distributed computing system with task allocation using simple genetic algorithm. *Journal of Systems Architecture*, **47**, pp. 549-554.

Yang, J-E., M-J. Hwang, T-Y. Sung and Y. Jin (1999). Application of genetic algorithm for reliability allocation in nuclear power plants, *Reliability Engineering and System Safety*, **65**, pp. 229-238.

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