CHEMICAL ENGINEERING TRANSACTIONS, Volume 3, 2003
Edited by Sauro Pierucci
Copyright © 2003, AIDIC Servizi S.r.l., ISBN 88-900775-2-2

Optimal Safety Control System Design

Graciela Noya[1], Mabel Sánchez[2*] and Alberto Bandoni[2]
[1] Universidad Nacional de la Patagonia S.J.Bosco
[1] Km 4 - (9000) - Comodoro Rivadavia ARGENTINA
[2] Planta Piloto de Ingenieria Química (UNS – CONICET)
[2] Camino La Carrindanga Km 7 - (8000) Bahía Blanca ARGENTINA

This paper is focused on the optimal design of Safety Instrumented Systems. A combinatorial optimisation problem is formulated that involves as design variables the architecture and type of components of the three subsystems (sensors, logic solvers, final elements) and their test intervals. The life cycle cost is minimized subject to safety and spurious trip constraints. An evolutionary technique based on Genetic Algorithms is presented to solve the problem. Application results are reported for case studies.

1. Introduction

If existing protective layers are insufficient to prevent a potential hazard, the installation of a Safety Instrumented System (SIS) is next considered. The SIS reads sensors, does the calculations required to recognize potentially dangerous events, and produces an output to actuators to mitigate the dangerous situation. Because international standards on SIS's design are performance oriented rather than prescriptive, the designer should select the SIS's acceptable level of risk, called Safety Integrity Level (SIL), and then specify the system architecture, maintenance works, test intervals, etc., in order to satisfy the required SIL. An iterative design procedure is followed until the SIL is verified. In this context, the optimal design of SIS's emerges as an attractive way to perform the selection efficiently.

The optimal evaluation of discrete test intervals for fixed architectures was reported by Martorell et al. (2000) and Giuggioli et al. (2001), that provided optimization criteria in terms of cost and availability. Recently a general formulation for the optimal SIS design is presented in Noya et. al (2003), where it is proposed to minimize the SIS life cycle cost subject to SIL and probability of safe failure constraints. The structure of redundant components and discrete test intervals of each subsystem are considered simultaneously as design variables.

In this work the aforementioned optimal SIS design formulation is extended to incorporate both redundant and diverse components in subsystem architectures. The number of alternative arrangements to be analysed increases significantly because subsystems are built selecting components from a discrete set of different elements, which can be accommodated in redundant or diverse architectures. Also test intervals constitute a discrete set. Due to the combinatorial nature of the optimization problem, an evolutionary strategy of solution is proposed based on Genetic Algorithms, that satisfactorily approaches the optimal solution. The paper is structured as follows. In the next section the formulation of the optimal SIS design for diverse component structures is formulated. Then the proposed solution procedure is presented , followed by a section that contains application results for case studies. Finally conclusions and future research work are addressed.

2. Optimal Design of Safety Instrumented Systems

A SIS consists of sensors, controllers and final elements that work together to provide the safety function. Each subsystem is made up of components that can be configured in different architectures. Goble (1998) provides a good survey of these arrangements. Moreover, configuration components can be selected from a set of discrete elements with particular failure rates, maintenance and cost features. Consequently redundant (equal components) and diverse (different components) structures are generated.

In this work the optimal SIS design for redundant and diverse subsystems is formulated as a constrained optimization problem. The objective function is the life cycle cost of the three subsystems that composed the SIS. Regarding the constraints, safety or environmental control is important but so is the economic impact of spurious trips, which are not always nuisance events. In consequence, SIS average probability of failure on demand (PFD$_{SIS}$) and SIS average probability of spurious trips (PFS$_{SIS}$) are incorporated as restrictions. They are calculated in terms of the contributions from each subsystem. Problem formulation is as follows

$$Min\left[\sum_{k=1}^{K}\sum_{i=1}^{NSS}\sum_{j=1}^{C(NS,J_i^s)} LCC_{kij}^{s}\, H_{kij}^{s} + \sum_{k=1}^{K}\sum_{i=1}^{NCS}\sum_{j=1}^{C(NC,J_i^c)} LCC_{kij}^{c}\, H_{kij}^{c} + \sum_{k=1}^{K}\sum_{i=1}^{NFS}\sum_{j=1}^{C(NF,J_i^f)} LCC_{kij}^{f}\, H_{kij}^{f}\right]$$

$$\begin{aligned} &s.t. \\ &\quad PFD^s(H_{kij}^s)+PFD^c(H_{kij}^c)+PFD^f(H_{kij}^f)<PFD* \\ &\quad PFS^s(H_{kij}^s)+PFS^c(H_{kij}^c)+PFS^f(H_{kij}^f)<PFS* \end{aligned} \tag{1}$$

where:

K = number of discrete time intervals of inspection TI

NSS, NCS and NFS = number of feasible architectures selected for sensors, controllers and final elements

$C(NS,J_i^s)$ = number of arrangements of NS available sensors, such that the total number of sensors of configuration i (J_i^s) is verified, considering cases of redundant and diverse structures.

$C(NC,J_i^c), C(NF,J_i^f)$ = idem $C(NS,J_i^s)$ for controllers and final elements

LCC_{kij}^s = sensor subsystem life cycle cost evaluated considering k-th inspection interval, i-th sensor architecture and j-th sensor arrangement.

LCC_{kij}^c , LCC_{kij}^f = = idem as LCC_{kij}^s for controllers and final elements

H_{kij} = binary variable, H_{kij}=1 means the corresponding LCC_{kij} participates in SIS's cost, H_{kij}=0 otherwise.

The life cost of each subsystem is defined as the sum of the procurement cost *(PC)* cost and the present value of the ownership cost (*OC*) considering a life period of *n* years

$$LCC = PC + \sum_{i=1}^{n} \frac{OCy}{(1+R)^{i}} = PC + \sum_{i=1}^{n} \frac{(FC + CMC + CT + CCMC + CCT + RC + FTC)}{(1+R)^{i}} \quad (2)$$

where R = discount rate; Ocy = annual cost of ownership; FC = Fixed Operation cost (consumption and fixed maintenance costs); CMC = Corrective Maintenance Cost, cost associated with the repair of failures detected before inspection; CT = Test Cost, cost of SIS inspection at intervals *TI* and the repair cost of failures found during test. Moreover, if a process demand occurs and the SIS is unavailable due to repair tasks or test, a dangerous condition arises. Thus there exist Consequence Costs associated with the corrective maintenance (*CCMC*) and test (*CCT*). A dangerous situation also appears if the SIS fails in a dangerous undetected way. A Risk Cost (*RC*) is associated with the occurrence of this event. In addition, the cost of a false trip (*FTC*) should be evaluated, because it generates start-up operations, which are less safe conditions than normal operation, and production downtime costs.

Expressions to calculate the cost terms involved in *Ocy* are provided in Noya (2003). Except *FC*, they depend on subsystem probability of being in a partially or fully degraded state. For example, *CMC* is calculated using the average probability of being in a detected partially or fully degraded state over *TI*, and *RC* is evaluated in terms of the average probability of being in an undetected fully degraded state.

Markow models are applied to evaluate the aforementioned probabilities. Each architecture is represented by a Markov diagram (Goble, 1998) and state evolutions are calculated between t=0 and t=*TI*, then average probabilities for intermediate and final states are evaluated at *TI*. The model assumes constant failures rates and repair rates, safe and dangerous modes of failure, on-line diagnostic capabilities and common cause, quick repair of detected system failures without shutting down the process and perfect inspection and repair.

In this work, state probabilities for diverse architectures are calculated using the same redundant-architecture Markov models, but transitions between states are modified to take into account different individual failure rates as follows,
a) the product of equal failure rates is replaced by the sum of the individual ones
b) single failure rates are changed by the maximum failure rate among all components
c) the product of two equal failure rates in 2oo3 architectures is swapped by the maximum sum of failure rates among all pairs of components.

To evaluate PFD for each architecture, the SIS unavailability due to testing and repair tasks for failures found during test is added to the average unavailability on demand over *TI* obtained using Markov models. The PFS is calculated as the average probability of being in the safe state over *TI*.

3. An Evolutionary Solution Procedure

The proposed formulation of the optimal SIS design results in a combinatorial optimisation problem. Stochastic methods arise as a good alternative to tackle them, and among these techniques, Genetic Algorithms (GA) have been extensively explored for the resolution of problems involving decisions about the structure or sequence of chemical engineering process. Consequently, an evolutionary technique based on GA is developed to solve it.

An evolutionary technique is a probabilistic algorithm that maintains a population of individuals $P(t)=\{p_1(t), p_2(t),...\}$ for iteration *t*. Each individual represents a potential solution to the problem. Each solution p_i^t is evaluated to give some measure of its fitness. Then a new population (iteration *t*+1) is formed by selecting the individuals that fit better. Some members of the new population undergo transformations by means of genetic operators to form new solutions. There are unary transformations (mutation) which produce new individuals by a small change on a single individual, and higher order transformations (crossover) which form new individuals by combining parts from several individuals. The program converges after some number of generations. The best individual is considered a near optimum solution (Michalewicz, 1996).
For the optimal SIS design, the relevant features of the new evolutionary procedure are considered next.

3.1 Solution Representation and Initial Population

An individual is represented by a string of discrete numbers that follows the order indicated in Fig. 1. The first position corresponds to sensor architecture index (i^s=1:*NSS*). A block of *NS* integers that can take values between 0 and 3 follows. A zero value indicates the component is not present in the architecture, a non-zero value represents how many components of this type participate in the arrangement. The representation is repeated for controllers and final elements. The last three positions correspond to the interval test index for each subsystem.

An initial population is randomly generated for each subsystem architecture. The blocks of *NS*, *NC* and *NF* components are also filled randomly, but taking into account that the amount of components of each subsystem should be satisfied.

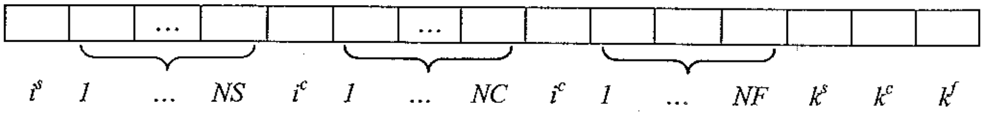

Fig.1: *Chromosome representation*

3.2 Fitness evaluation

In this work the constraint handling approach proposed by Deb(1998) is applied. The fitness function is defined as the SIS life cycle cost for a feasible solution. Otherwise, it is obtained adding the constraints violations to the highest objective function value of all feasible solutions for the current generation.

3.3 Genetic Operators

The selection of some individuals from the population to be parents in the reproduction stage is conducted using the ranking method, considering the selective pressure parameter equal to 0.08. Regarding the crossover and mutation operators, Simple Crossover and Uniform Mutation are applied. The corresponding probability parameters are 0.6 and 0.1 respectively.

4. Case Study

In this section a case study is presented to show the application of the proposed evolutionary strategy. Let us suppose the hardware components in Table 1 constitute the candidate set of elements to become part of the SIS subsystems under design. In this table, λ represents the total failure rate and C^d, the coverage factor of dangerous failures. Another parameters used to categorize the different types of failure rates are the following:

a) % safe failures for sensors and controllers = 50%

b) % safe failures for final elements = 80%

c) Common Cause β factor for redundant architectures = 0.05, 0.03 and 0.10 for sensors, controllers and final elements respectively. These values reduces to 0.025, 0.01 and 0.05 for diverse architectures.

d) Regarding the parameters involved in cost function, PFD and PFS evaluation, see Noya et al. (2003) for details.

e) The set of discrete allowable inspection times considered in this example is [4320 8760 13140 17520]h and is fixed for all the subsystems.

Runs are conducted for PFS=0.1 and PFD={0.01, 0.001}, considering a downtime cost CLP=500 \$/h and the cost of a dangerous event, Crisk = 1e6\$. Results are reported in Table 2 and Table 3.

Table 1: Hardware Elements

Sensors			Controllers			Final Elements		
λ	C^d	Cost	λ	C^d	Cost	λ	C^d	Cost
$[f/h]x10^6$		\$	$[f/h]x10^6$		\$	$[f/h]x10^6$		\$
2.85	0.9	400	5.00	0.98	6000	10.0	0.8	400
5.70	0.5	180	1.30	0.98	15000	13.0	0.0	250

Table 2: Optimal SIS structure

	Sensors			Controllers			Final Elements			Cost
PFD	Arch.	Type 1	Type 2	Arch.	Type 1	Type 2	Arch.	Type 1	Type 2	$
0.01	1oo2D	0	2	1oo1	1	0	2oo2	2	0	20726
0.01	1oo2D	2	0	1oo2D	2	0	1oo2	2	0	43451

Table 3: Optimal Test Interval

PFD	TI^s	TI^c	TI^f
0.01	8760	13140	4320
0.001	17520	17520	13140

5. Conclusions

In this paper, the optimal SIS design for redundant and diverse subsystems is formulated. The SIS life cycle cost is minimized subject to constraints that take into account both safety and the impact of spurious trips. To consider diverse subsystems, a methodology is proposed to calculate the state probabilities of Markov Models. Regarding problem solution, an evolutionary strategy is developed to solve the resulting combinatorial problem. It successfully approaches towards the optimal solution.

Future work will addressed the impact on the design of imperfect repair and test tasks.

6. References

Deb K., 1998, An efficient constraint handling method for genetic algorithms, Comp. Meth. Appl. Mech. Eng.

Giuggioli P., M. Marseguerra, and E. Zio, 2001, Application of Genetic Algorithms to the Multiple Objective Optimization of the Inspection Times of a Safety System of a Pressurized Water Reactor, 1052-1060, ESREL 2001 Conference, Torino, Italy.

Goble, W., 1998, Control Systems Safety Evaluation & Reliability, ISA.

Noya, G., M. Sánchez and A. Bandoni, Reliability and Cost Issues in Safety Control System Design (2003), Spring AIChE Conference, New Orleans, USA.

Martorell S., Carlos S., Sánchez A. and Serradell V., 2000, Constrained optimization of test intervals using a steady state Genetic Algorithm, Reliability Engineering and System Safety, 67, 215-232.

Michalewicz Z., 1996, Genetic Algorithms + Data Structures = Evolution Programs; Springer