Grid–sampling optimisation of safety systems

Grid–Sampling Optimisation of Safety Systems

Prof. J.D.Andrews & Dr. L.M.Bartlett;

Department of Mathematical Sciences; Loughborough University; Loughborough; Leicestershire;UK

Keywords: Optimisation, Safety Systems, Fault Tree Analysis, Binary Decision Diagrams

Abstract

Safety systems are usually the last line of defence against the occurrence of a potentially hazardous event. Failure of a safety system on a potentially hazardous industrial system or process may have severe consequences. For a system whose failure could result in fatality it could be accepted that a merely adequate level of system unavailability is not sufficient. The aim should be to produce the optimal performance attainable within the constraints imposed on resources.

This paper investigates a design optimisation scheme that is appropriate for safety systems. The methodology presented in this paper adopts the latest improvements to the fault tree analysis technique, the binary decision diagram approach, to analyse the individual system designs. The grid-sampling optimisation technique is used to generate the final design specification with the constraints incorporated. To demonstrate the practicality of the method it has been applied to a High Integrity Protection System. In all there are 42,831,360 combinations of twelve design variables. There are three constraints imposed on the system in terms of cost, mean down time, and spurious trip frequency.

Introduction

Typically the design of a safety system follows the traditional process of preliminary design, analysis, appraisal and redesign. If, following analysis, the initial design does not meet some pre-determined acceptability criteria for system unavailability, deficiencies in the design are removed and the analysis and appraisal stages are repeated. Once the predicted system unavailability of the design reaches the acceptability criteria the design process stops and the system is adopted. However, for a system whose failure could result in fatality it could be accepted that a design which produces optimal performance not just an adequate level of performance is required.

The complexity of making a trade-off between system performance requirements and compliance with imposed constraints makes it highly unlikely that the design parameters can be manually selected such that optimal system performance can be achieved within the available resources. For this reason an optimisation algorithm integrated within the design process is required. An approach by which optimal performance can be obtained using the fault tree analysis method to determine the availability of each system was first introduced in 1994 “(ref. 1)”. This approach has since been modified and improved by using Binary Decision Diagrams “(ref. 2-6)”, the latest development in the Fault Tree Analysis technique. The latter method incorporated the use of a Genetic Algorithm “(ref. 7-8)” to perform the optimisation, allowing a number of design alternatives to be investigated simultaneously. This paper investigates an alternative optimisation algorithm, referred to as the grid-sampling optimisation technique, to produce an optimal design for a high integrity safety system, given set constraints.

Safety System Design - The High Integrity Protection System

The function of the high integrity protection system (HIPS) is to prevent a high-pressure surge passing through the system. In this way protection is provided for processing equipment whose pressure rating would be exceeded. The high pressure originates from a production well of a not normally manned offshore platform and the pieces of equipment to be protected are vessels located downstream on the processing platform. The basic features of the protection system are shown in figure 1.

Originally published by the System Safety Society, in the Proceedings of the20th International System Safety Conference, held at Denver, August 2002

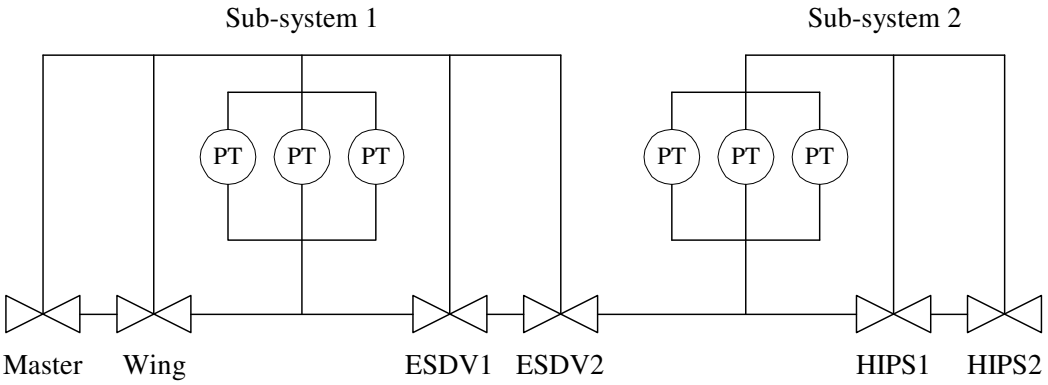

Figure 1 - High Integrity Protection System

The first level of protection is the ESD (emergency shutdown) subsystem. Pressure in the pipeline is monitored using pressure transmitters (PT's). When the pipeline pressure exceeds the permitted value then the ESD system acts to close the Wing and Master valves on the well together with any ESD valves that have been fitted. To provide an additional level of protection a second level of redundancy can be incorporated by the inclusion of a HIPS (high-integrity protection system). This works in a similar manner to the ESD system but is completely independent in operation.

Even with a relatively simple system such as this there are a vast number of options for the designer to consider. In this example it is required to determine values for the design variables that represent the following:

i)	How many ESD valves are required (0,1,2)?	E
ii)	How many HIPS valves are required (0,1,2)?	H
iii)	How many pressure transmitters for each subsystem (0,1,2,3,4)?	N_1, N_2
iv)	How many transmitters are required to trip?	K_1, K_2
v)	Which of two possible ESD/HIPS valves to select?	V_1, V_2
vi)	Which of two possible pressure transmitters to select?	P_1, P_2
vii)	Maintenance test interval in weeks for each subsystem (1 week – 2 years)?	θ_1, θ_2

Table 1 - Component Data

Component	Dormant Failure Rate	Dormant Mean Repair Time	Spurious Failure Rate	Spurious Mean Repair Time	Cost	Test time
Wing Valve	1.14×10^{-5}	36.0	1×10^{-6}	36.0	100	12
Master Valve	1.14×10^{-5}	36.0	1×10^{-6}	36.0	100	12
HIPS1	5.44×10^{-6}	36.0	5×10^{-7}	36.0	250	15
HIPS2	1×10^{-5}	36.0	1×10^{-5}	36.0	200	10
ESDV1	5.44×10^{-6}	36.0	5×10^{-7}	36.0	250	15
ESDV2	1×10^{-5}	36.0	1×10^{-5}	36.0	200	10
Solenoid Valve	5×10^{-6}	36.0	5×10^{-7}	36.0	20	5
Relay Contacts	0.23×10^{-6}	36.0	2×10^{-6}	36.0	1	2
PT1	1.5×10^{-6}	36.0	1.5×10^{-5}	36.0	20	1
PT2	7×10^{-6}	36.0	7×10^{-5}	36.0	10	2
Computer Logic	1×10^{-5}	36.0	1×10^{-5}	36.0	20	1

Limitations have been placed on the design such that:

1. The total system cost must be less than 1000 units. Hardware costs are given in table 1.

2. The average time each year that the system resides in the down state due to preventive maintenance must be less than 130 hours. Times taken to service each component at each maintenance test are also shown in table 1.
3. The number of times that a spurious system shutdown occurs would be unacceptable if it was more than once per year.

Protection System Analysis

Analysing The Design: A criterion must be determined to quantify how "good" each system design actually is. The most important feature of a safety system is that it works when the demand arises. The objective is, therefore, to minimise system unavailability (i.e. the probability of system failure on demand) and as such this provides a measure of system performance. Consideration must also be given, however, to the available resources. The HIPS is limited by cost, maintenance effort and spurious trip frequency. The design options need to be adjusted in order to improve system performance without violating the constraints.

Therefore, to assess the performance of a potential system design the system unavailability needs to be considered along with the limitations that are placed on the system. Thus, the performance depends on four parts:

1. The probability of system failure (unavailability, Q_{SYS}).
2. A penalty for the design exceeding the total cost constraint (C_{pen}).
3. A penalty for exceeding the total maintenance down time constraint (MDT_{pen}).
4. A penalty for exceeding the spurious trip constraint (ST_{pen}).

The result is a sole value to represent system performance for each design, referred to as the penalised system unavailability of the design, Q'_{SYS}. If a particular design exceeds any of the stated limits, the respective penalty is added to the system unavailability of the design in question "(eq. 1)".

$$Q'_{SYS} = Q_{SYS} + C_{pen} + MDT_{pen} + ST_{pen} \quad (1)$$

In order to assess each design option a means to evaluate each term in equation 1 is required. This is discussed in the following sections.

Evaluating System Unavailability: No explicit objective function can be formulated. Incorporating an added level of redundancy within the system would require a new term to be added to the objective function, therefore altering its characteristics entirely. As such, fault trees are used to quantify the system unavailability of each potential design. It is however, a time consuming, impractical task to construct a fault tree for each design variation. To resolve this difficulty house events "(ref. 1)" can be used to enable the construction of a single fault tree capable of representing causes of the system failure mode for each possible system design. House events in the fault tree, which are either TRUE or FALSE, are utilised to switch on or off different branches to model the changes in the causes of failure for each design alternative.

Analysis of the fault tree structure is evaluated using the Binary Decision Diagram Approach "(ref. 2 – 6)", which can introduce significant advantages into the quantitative process. Quantitative calculations do not require the determination of the minimal cut sets and the top event parameters are calculated exactly. Q_{SYS} is calculated from the system fault tree using component failure and repair data given in table 1.

Cost and Mean Down Time (MDT) Evaluation: Constraints fall into two categories, explicit constraints; those that can be determined from an explicit function of the design variables and are, therefore, easily evaluated, and implicit constraints; those that can not be expressed as a function and can only be evaluated by full analysis of the system.

Cost and MDT are explicit constraints. Total cost is the sum of the cost of subsystem 1 and subsystem 2, and is represented by equations 2 – 4.

$$COST = COST(SUBSYS1) + COST(SUBSYS2) \leq 1000 \quad (2)$$

$$COST(SUBSYS1) = E(V_1C_{V1} + V_2C_{V2} + C_S) + N_1(P_1C_{P1} + P_2C_{P2}) + 261 \quad (3)$$

$$COST(SUBSYS2) = H(V_1C_{V1} + V_2C_{V2} + C_S) + N_2(P_1C_{P1} + P_2C_{P2}) + 21 \quad (4)$$

where C_{V1} and C_{V2} are the cost of the two valve types, C_{P1} and C_{P2} represent the cost of the two pressure transmitter types and C_S is the cost of the solenoid valve.

Subsystem 1 includes a wing and master valve, their solenoid valves, the computer and relays, hence, the fixed cost of 261 units is included in equation 3. The extra cost depends on the number and type of ESD valves and the number and type of pressure transmitters. Subsystem 2 has a fixed cost of 21 units due to the computer and control relays, hence the constant in equation 4.

Similarly average MDT for preventive maintenance is a sum of subsystem 1 and subsystem 2, as given by equations 5 – 7.

$$MDT = MDT(SUBSYS1) + MDT(SUBSYS2) \leq 130 \quad (5)$$

$$MDT(SUBSYS1) = \frac{52}{\theta_1}[E(V_1M_{V1} + V_2M_{V2} + M_S) + N_1(P_1M_{P1} + P_2M_{P2}) + 47] \quad (6)$$

$$MDT(SUBSYS1) = \frac{52}{\theta_2}[H(V_1M_{V1} + V_2M_{V2} + M_S) + N_2(P_1M_{P1} + P_2M_{P2}) + 13] \quad (7)$$

where M_{V1} and M_{V2} represent the test times of the two valve types, M_{P1} and M_{P2} are the test times of the two pressure transmitter types, and M_S is the test time of the solenoid valves.

The constant 47 in equation 6 is the test time for the wing and master valve, their solenoids, the computer and the control relay for subsystem 1. The test time for the computer and control relay for subsystem 2 is 13 units, as stated in equation 7.

Spurious Trip Evaluation: Spurious trip frequency of the HIPS is an example of an implicit constraint, this is evaluated in a similar manner to the system unavailability. The specific fault tree relating to the spurious activation of the HIPS is constructed for each potential design by incorporating House events. Relevant House events are set for each specific design considered. The top event will occur if any one of the valves included along the pipeline closes spuriously. The resulting fault tree is again analysed using the BDD methodology.

Grid – Sampling Optimisation

Introduction: This optimisation technique works on the basis that some form of objective function is assumed to estimate the system unavailability and a region defined over which this approximate function is considered accurate. An initial design is chosen and an objective function derived such that it is feasible within a restricted neighbourhood of the initial design point. In a similar manner, a function is derived which is assumed to accurately represent the spurious trip frequency within the restricted neighbourhood. An efficient, computerised procedure can then analyse each point within the restricted design space to obtain the enclosed optimal design. A new neighbourhood is then constructed around the new design point and the process is repeated.

The procedure results in an iterative scheme where the optimal solution is approached by solving a sequence of optimisation problems. Each problem in the sequence produces a new improved solution and the next problem to solve is defined by moving the feasible solution space to the neighbourhood surrounding the new solution re-defining and re-evaluating the approximate objective functions.

Overview of The Optimisation Algorithm: An initial design is produced by the design engineer, denoted by $\boldsymbol{x}^0$. It is then ensured that the chosen design does not violate the MDT, cost or spurious trip limitations. If any of these constraints are violated a new start point is selected. The design's system unavailability is calculated, using the BDD technique.

Forms of the objective function, for both the system unavailability and spurious trip frequency, are assumed and a restricted neighbourhood defined within which these functions are assumed accurate. Each potential design vector identified within the restricted space is subsequently analysed automatically using the approximate objective function and spurious trip function along with the explicit formulae for cost and MDT.

The system unavailability of the best predicted point resulting from the restricted search, denoted by Q_{SYS}^{P} is compared with the system unavailability of the initial design Q_{SYS}^{j}. If the predicted point shows potential for improvement it is accepted for further consideration and defined as $\boldsymbol{x}^{j+1}$, where j is the iteration number (initially set to 0) and denotes the number of predicted designs that are accepted. The actual values of F_{SYS}^{j+1} (spurious trip frequency) and Q_{SYS}^{j+1} are evaluated using the appropriate BDD. If the spurious trip rate is less than 1 and the system unavailability verifies the improvement over the previous design, the new design point is accepted. If either the spurious trip is greater than 1 or the system unavailability is greater than Q_{SYS}^{j}, the predicted point is rejected. In such circumstances, the current design point ($\boldsymbol{x}^{j}$) is retained, the boundaries of the restricted neighbourhood of the search space are reduced, and the search process repeated within the reduced restricted neighbourhood. The restricted search space is continually reduced until either the actual performance values of a predicted design show improvement over the current design or the boundaries about the search space are reduced to contain only the current point. The latter scenario terminates the algorithm and the current vector is deemed the most optimal design. At any point the algorithm terminates if the search within the restricted neighbourhood fails to predict a design which shows improvement over the current best. The resulting optimal design is, therefore, $\boldsymbol{x}^{j}$.

Formulation of The Objective Function: To explore the design space around the initial design and progress to an improved point a means to express the system performance as a function of the design is required, i.e. $Q_{SYS} = f(\boldsymbol{x})$ where $\boldsymbol{x}$ = (E, N_1, K_1, H, N_2, K_2, V, P, θ_1, θ_2). Assumption of an objective function form uses the Taylor expansion about the current design point ($\boldsymbol{x}$) "(eq. 8)".

$$f(\boldsymbol{x}+\Delta\boldsymbol{x}) = f(\boldsymbol{x}) + g^{T}\Delta\boldsymbol{x} + \frac{1}{2}\Delta\boldsymbol{x}^{T} H \Delta\boldsymbol{x} + \ldots \tag{8}$$

where $\Delta\boldsymbol{x}$ is the change in the design vector, g the gradient vector and H the Hessian matrix. Taylor series approximates the value of points sufficiently close to x, however, there is no function that can represent $f(\boldsymbol{x} + \Delta\boldsymbol{x})$ for the entire design space.

Linear truncation of the Taylor expansion means that $f(\boldsymbol{x} + \Delta\boldsymbol{x})$ can be evaluated providing that the gradient vector can be obtained. That is $\partial f / \partial x_i$ for each design parameter, where the partial derivatives show the rate of change of system performance with respect to the respective parameter. Strictly formulation of $\partial f / \partial x_i$ can not occur as integer variables are being considered. To overcome this it is assumed that a smooth curve has been used to link all discrete points to give the marginal distribution of f as a function of $\boldsymbol{x}$, then $\partial f / \partial x_i$ can be obtained for the smooth curve.

Finite differences can be used to estimate $\partial f / \partial x_i$. For a linear objective function the partial derivatives are evaluated to specify the terms in the function using the central difference formula if possible "(eq. 9)".

$$\frac{\partial Q_{SYS}}{\partial x_i} = \frac{Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i + dx_i, x_{i+1}, \ldots, x_n) - Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i - dx_i, x_{i+1}, \ldots, x_n)}{2dx_i} \tag{9}$$

The BDD is used to obtain $Q_{SYS}(x_i + \mathrm{d}x_i)$ and $Q_{SYS}(x_i - \mathrm{d}x_i)$ for each variable, provided $x_i + \mathrm{d}x_i$ and $x_i - \mathrm{d}x_i$ represent physically possible designs. If one of the variable x_i values is infeasible, this is overcome using either the forward or backward scheme, equation 10 or 11 respectively.

$$\frac{\partial Q_{SYS}}{\partial x_i} = \frac{Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i + dx_i, x_{i+1}, \ldots, x_n) - Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n)}{dx_i} \tag{10}$$

$$\frac{\partial Q_{SYS}}{\partial x_i} = \frac{Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_n) - Q_{SYS}(x_1, x_2, \ldots, x_{i-1}, x_i - dx_i, x_{i+1}, \ldots, x_n)}{dx_i} \tag{11}$$

The range of the parameter being dealt with and its value in the current design determines the difference scheme used. Boolean variables, i.e. V and P, are necessarily restricted to either forward or backward differences. The algorithm in figure 2 illustrates the estimation of partial derivatives for E, the parameter governing the number of ESD valves with range 0 to 2. Incrementing a parameter value within its range may still render a design infeasible due to interactions with other parameters. Consider for example, a *k*-out-of-*n* voting system design with $N_1 = K_1 = 4$. Estimating the partial derivative with respect to N_1 uses backward differences. However, $N_1 = 3$ and $K_1 = 4$ is infeasible. To overcome this K_1 must also be modified.

If E = 0
    Evaluate $Q(x_{E+1}, \mathbf{x})$
    Evaluate partial derivative using forward differences
If E = 1
    Evaluate $Q(x_{E+1}, \mathbf{x})$
    Evaluate partial derivative using central differences
If E = 2
    Evaluate $Q(x_{E-1}, \mathbf{x})$
    Evaluate partial derivative using backward differences

Figure 2 - Algorithm For Governing Number of ESD Valves

Problems arise when the design under consideration has no redundant system, i.e. H = 0. Utilising forward differences to determine the partial difference with respect to H increments H by 1. To ensure the resulting design is feasible N_2, K_2 and θ_2 can not remain at 0. To overcome this the forward difference scheme is applied to an alternative design with $H = N_2 = K_2 = 1$ and $\theta_2 = 50$ to estimate $\partial Q_{SYS} / \partial H$.

Having evaluated each derivative the linearly truncated Taylor expansion takes the form given in equation 12, which defines the objective function for system unavailability.

$$Q_{SYS}(x + \Delta x) = Q_{SYS}^{j} + \sum_{i=1}^{n} \left(\frac{\partial Q_{SYS}}{\partial x_i} \right)^{j} dx_i \tag{12}$$

The objective function to approximate the frequency of spurious system failure is derived in an identical manner.

Limiting The Scope of The Objective Function: The nature of the HIPS system restricts the design space. Specific ranges allocated to design variables define upper and lower bounds. Constraint functions remove other design alternatives. Additionally, since the variables must assume integer values, only integer points within the design space are feasible.

Linear truncation of the Taylor series enables only an approximation of $Q_{SYS}(\mathbf{x} + \Delta\mathbf{x})$. As such, a restricted solution space in the neighbourhood of the current point, where the approximate solution is deemed to be acceptably accurate, must be defined. To enforce the restricted neighbourhood the range of each variable is limited further through the introduction of additional constraints"(eq.13)":

$$x_i^j - \Delta x_{iL} \le x_i^T \le x_i^j + \Delta x_{iU} \tag{13}$$

where x_i^T represents the variable of a design point within the restricted space, x_i^j represents design variable at the j^{th} accepted design point and Δx_{iL} and Δx_{iU} are the lower and upper limits by which x_i is allowed to change. Where possible these constraints are set one unit either side of the current value of the design variable. The MDT parameters are an exception. The range of values covered by the test parameters is much greater and hence, has scope to relax strict bounds is more flexible. Initial bounds are set 12 units (weeks) either side of the actual test interval values for the j^{th} design.

Reducing The Restricted Design Space: The bounds to be reduced refer only to the restricted range about the parameters. Each consecutive time a predicted improvement ($Q_{SYS}^{j+1} > Q_{SYS}^{j}$) proves invalid from the BDD analysis, the distance of the enforced upper and lower bound about the actual parameter value is reduced. If the restricted design space results in the newly established not differing from $\boldsymbol{x}^j$ the algorithm is terminated and $\boldsymbol{x}^j$ is deemed to the optimal design.

Application of The Grid Sampling Method to System Analysis

The above algorithm has been applied to the HIPS. The initial design is stated in the second column of table 2. The following columns state the consecutive designs, which were predicted to show improvement

Table 2 - Characteristics of Each Predicted Design

Design No	Initial Design	1	2	3	4	5	6	7	8	9
Design Accept		**1**			**2**					
E	1	**0**	0	0	**0**	0	0	0	0	0
K_1/N_1	2/2	**1/3**	2/2	2/2	**2/3**	1/4	1/4	1/4	1/4	1/4
H	1	**1**	2	2	**2**	2	2	2	2	2
K_2/N_2	1/1	**2/2**	1/3	1/3	**1/3**	1/2	2/2	2/2	2/2	2/3
V	1	**1**	2	2	**2**	2	2	2	2	2
P	1	**1**	1	1	**1**	1	1	1	1	1
θ_1	40	**30**	30	28	**27**	30	31	28	27	28
θ_2	50	**39**	30	33	**36**	31	30	34	36	35
Q'_{SYS}	3.95 e-3	**9.34 e-4**	9.35 e-4	9.62 e-4	**7.97 e-4**	9.69 e-4	9.7 e-4	9.91 e-4	1.01 e-4	8.04 e-4
F_{SYS}	0.420	**0.942**	0.847	0.847	**0.847**	0.977	0.977	0.977	0.977	0.976
MDT	101.66	**129.3**	130	129.16	**129.04**	129.78	129.4	129.67	129.52	129.63
Cost	882	**922**	822	822	**842**	842	842	842	842	862

over the current design. Those designs that were accepted when their actual performance measures were evaluated are represented in bold. As can be seen, the first design is accepted as an improvement over the initial vector is that predicted 1st. The most optimal design from the grid sampling process using the specified initial design is described in the 6th column, headed "Design No. 4".

The constraint values associated with each design are stated in the final three rows of table 2. The values predicted for system unavailability and spurious trip frequency are also given. The initial design has a system unavailability of 3.95×10^{-3}. The system unavailability of the final design shows vast improvement specifying a value of 7.97×10^{-4}.

An objective function is first assumed about the initial design to approximate both the system unavailability and spurious trip frequency. Table 3 states the gradient vector values and the difference scheme used for each parameter for each failure mode (F, B and C denote forward difference, backward difference and central difference respectively). In addition, the upper and lower bounds of the restricted neighbourhood established about each parameter are specified. (if the HIPS valve is set to 0 parameters N2, K2 and theta 2 are modified accordingly).

The restricted neighbourhood about the initial design ($\boldsymbol{x}^0$) was analysed and an improved design predicted. The actual performance values associated with this predicted design proved to be both feasible and fitter than the initial vector, giving rise to $\boldsymbol{x}^1$. A new neighbourhood and a second objective function was consequently established about $\mathbf{x}^1$.

The restricted neighbourhood about $\boldsymbol{x}^1$ was analysed and an improved design predicted. The actual system unavailability of this design proved less fit than Q_{SYS}^1 and was, therefore, rejected. The MDT boundaries were reduced to $24 \le \theta_1 \le 36$ and $33 \le \theta_2 \le 45$ and this reduced neighbourhood re-analysed. Similarly the next predicted design proved less fit and the MDT boundaries were further reduced to $27 \le \theta_1 \le 33$ and $36 \le \theta_2 \le 42$. A further analysis of the area produced a design whose actual values showed improvement over Q_{SYS}^1 and was therefore accepted, giving rise to $\boldsymbol{x}^2$. The feasible solution space was moved to the neighbourhood surrounding this new solution with variable bounds reset to their original size limits and the objective function coefficients re-evaluated. Analysis of the region surrounding $\boldsymbol{x}^2$ produced 5 consecutive designs predicted to improve Q_{SYS}^2. The actual system unavailability of each prediction proved, however, to be inferior. Following the fifth prediction the bounded interval had been maximally reduced and the algorithm is terminated. The most optimal design resulting from this test was $\boldsymbol{x}^2$.

Table 3 - Objective Function Coefficients Associated With $\boldsymbol{x}^0$

Parameter	Difference scheme	Spurious $\partial F_{SYS} / \partial x_i$	Unavailability $\partial Q_{SYS} / \partial x_i$	Upper bound	Lower bound
E	C	8.73e-3	-1.30e-4	0	2
N_1	F	2.83e-4	-8.77e-4	1	3
K_1	B	-0.261	8.82e-4	1	3
H	F	8.73e-3	1.75e-3	0	2
N_2	F	0.131	2.54e-4	1	2
K_2	F	-0.262	5.07e-4	1	2
V	F	0.166	7.94e-4	1	2
P	F	0.482	4.90e-3	1	2
θ_1	C	0	9.73e-5	28	52
θ_2	C	0	7.59e-5	38	62

Results

The grid sampling approach was tested using eight alternative initial designs. Table 4 summarises the optimal design resulting from each run. Tests 1 to 6 produced a fitter design than initially chosen. The optimal designs resulting from tests 1, 2, 5 and 6 are very fit. A fitter design was not found on either test 7 or 8.

Table 4 - A Summary of the Best Design From Each Test Run

Test No	E	K1/N1	H	K2/N2	V	P	θ1	θ2	Q_{SYS}	F_{SYS}	Cost	MDT
1	0	2/3	2	1/3	2	1	27	36	7.97e-4	0.847	842	129
2	0	1/2	2	1/2	2	1	34	26	7.23e-4	0.977	802	129.6
3	0	2/2	2	1/2	2	1	31	29	9.34e-4	0.847	822	130
4	0	1/3	0	0/0	1	1	16	0	1.43e-2	0.411	301	126.7
5	0	1/2	2	1/2	2	1	38	24	7.5e-4	0.977	802	129.2
6	0	1/3	2	2/3	2	1	33	28	7.57e-4	0.847	842	129.9
7	0	2/3	1	1/3	1	1	40	40	2.51e-3	0.67	672	85.5
8	2	1/1	1	1/1	1	1	40	50	4.2e-3	0.807	982	108.2

Discussion of Results Using Linearised Grid Sampling Method

The optimisation procedure proves to be very effective if an appropriate initial design is chosen. Tests 2 and 5 produce very similar results, as shown in table 4. The only difference is that the maintenance allocated on the 5th test is not as effective. An unavailability of 7.57 x 10^{-4} results from the optimal design in the 6th test. This design differs from tests 2 and 5 in that both subsystems have 3 as opposed to 2 pressure transmitters and the HIPS subsystem is initiated by 2 of the 3 transmitters being activated. Although the cost is slightly more for the latter design, it may be preferred due the lower spurious trip rate.

Evident from the research was the dependency of the optimisation procedure on the initial design vector. The search is focussed about a single point in the entire design space. Search progresses toward the optimum area in the vicinity of the point. The result is that the method is somewhat local in scope.

In addition, problems arise due to interactions between parameter values rendering the design infeasible. The extreme case is when the HIPS valve is set to 0. As such, finite differences with respect to H require special treatment and incur greater accuracy in the numerical estimations. This is illustrated in test 4. The resulting design is comparatively poor. Inaccurate estimations of predicted designs in the restricted neighbourhood of the current point prevent more optimal points designs from being selected. This occurs to a lesser extent between other parameters, e.g. the number of pressure transmitters fitted and the number required to trip the system, and is possibly a factor in the poor performance of test 7 and 8.

In the main, the optimisation procedure enables full utilisation of the MDT resource, distributed across each sub-system to the best advantage. Bounds governing the feasible design over which the optimisation proceeds are relaxed for the test parameters. Greater exploration of the test parameter combinations for each design in the space, therefore ensues.

Acknowledgement

The authors would like to thank Dr. R. L. Pattison for her contribution to this paper.

References

1. J.D.Andrews, "Optimal Safety System Design using Fault Tree Analysis", Proc. IMechE, Vol. 208, 1994, pp123-131.
2. A.Rauzy, "New Algorithms for Fault Tree Analysis", Reliability Engineering and System Safety, Vol. 40, 1993, pp203-211.
3. R.M.Sinnamon, J.D.Andrews, "Fault Tree Analysis and Binary Decision Diagrams", Proceedings of 1996 Reliability and Maintainability Symposium, Las Vegas, Jan 1996, pp215-222.
4. R.M.Sinnamon, J.D.Andrews, "New Approaches to Evaluating Fault Trees", Proceedings of ESREL 95 Conference, June 1995, pp241-254.
5. R.M.Sinnamon, J.D.Andrews, "Improved Efficiency in Qualitative Fault Tree Analysis", Proceedings of the 12th ARTS, Manchester, April 1996.
6. R.M.Sinnamon, J.D.Andrews, "Improved Accuracy in Quantitative Fault Tree Analysis", Proceedings of the 12th ARTS, Manchester, April 1996.
7. J.D.Andrews, R.L.Pattison, "Optimal Safety System Performance", Proceedings of the Annual Reliability and Maintainability Symposium, Philadelphia, 13-16 Jan 1997, pp76-84.
8. R.L.Pattison, J.D.Andrews, "Genetic Algorithms in Optimal Safety System Design", IMechE Proceedings Part E, Journal of Process Mechanical Engineering, Vol. E3, 1999, pp187-197.

Biographies

John D Andrews; Department of Mathematical Sciences; Loughborough University; Loughborough; LE11 3TU; U.K. E-mail: J.D.Andrews@lboro.ac.uk.

Prof. J.D. Andrews is a Professor in the Department of Mathematical Sciences at Loughborough University. He joined this department in 1989 having previously gained nine years industrial research experience with British Gas and two years lecturing experience in the Mechanical Engineering Department at the University of Central England. His current research interests concern the assessment of the safety and risk of potentially hazardous industrial activities. This research has been heavily supported by industrial funding. Over recent years grants have been secured from the MOD, Rolls Royce Aero Engines, Mobil North Sea, and Bechtel. Professor Andrews has numerous journal/conference publications along with a jointly authored book "Risk and Reliability Assessment" which is now in its second edition.

Lisa M Bartlett; Department of Mathematical Sciences; Loughborough University; Loughborough; LE11 3TU; U.K. E-mail: L.M.Bartlett@lboro.ac.uk.

Dr. Lisa Bartlett is a lecturer in the Department of Mathematical Sciences at Loughborough University. She gained a first class honours degree in Mathematics and Sports Science (1997), and PhD in Fault Tree Analysis methods (2000) from Loughborough University. Her PhD research focused on the Binary Decision Diagram approach, and her current research interests continue in this area.