This item was submitted to [Loughborough's Research Repository](#) by the author.
Items in Figshare are protected by copyright, with all rights reserved, unless otherwise indicated.

Using statistically designed experiments for safety system optimization

PLEASE CITE THE PUBLISHED VERSION

PUBLISHER

© IMechE / Professional Engineering Publishing

LICENCE

CC BY-NC-ND 4.0

REPOSITORY RECORD

Bartlett, L.M., and J.D. Andrews. 2006. "Using Statistically Designed Experiments for Safety System Optimization". figshare. <https://hdl.handle.net/2134/2399>.

This item was submitted to Loughborough's Institutional Repository (<https://dspace.lboro.ac.uk/>) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to:
<http://creativecommons.org/licenses/by-nc-nd/2.5/>

Using statistically designed experiments for safety system optimization

J D Andrews and L M Bartlett*

Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, Leicestershire, UK

Abstract: This paper describes the method of statistically designed experiments (SDEs) which is used as a structured method to investigate the best setting for a number of decision variables in a system design problem. Traditionally, in the design of safety-critical systems, a trial and error type approach is undertaken to achieve a final system that meets the design objectives. This approach can be time consuming, and often only an adequate design is found rather than the optimal design for the available resources. Optimal use of resources should be imperative when possible lives are at risk. To demonstrate the practicality of this new structured approach for optimizing a safety system design, a high-integrity safety system has been used. Each design is analysed using the binary decision diagram analysis technique to establish the system unavailability, which is penalized if the system constraints are exceeded. System constraints indicate the limitations on the resources that can be utilized. The SDE approach highlights good and bad settings for possible design variables. This knowledge can then be used by more sophisticated search techniques. The latter part of this paper analyses the results from the best design generated using the SDE, for further optimization using localized optimization approaches.

Keywords: statistically designed experiments, fault tree analysis, binary decision diagrams, optimization, safety systems

NOTATION

C_{pen}	penalty for exceeding total cost constraint
ESD	emergency shutdown
HIPS	high-integrity protection system
MDT_{pen}	penalty for exceeding maintenance downtime constraint
Q_{sys}	system unavailability
Q'_{sys}	penalized system unavailability
SDE	statistically designed experiment
ST_{pen}	penalty for exceeding spurious trip constraint

1 INTRODUCTION

Safety systems are designed to operate when certain conditions occur and act to prevent their development into a hazardous situation. To minimize the risk the potential situation poses to members of the work force or public,

The MS was received on 18 March 2003 and was accepted after revision for publication on 23 September 2003.

**Corresponding author: Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, Leicestershire LE11 3TU, UK.*

it is essential that they have the maximum possible likelihood of working on demand for the resources available.

Techniques such as fault tree analysis [1], networks [2], Markov analysis [3] and simulation [4] are now commonly used for system availability assessment. However, they are usually used in the traditional engineering design process. This involves setting values of a potentially large number of decision variables, and then adjusting them either one at a time or by trial and error until an acceptable design performance is achieved. One criterion used to determine the adequacy of the design is a comparison with a predetermined target figure for its availability. This gives rise to an inefficient, unstructured design process, which will result in a design that is unlikely to make best use of available resources.

It is unlikely that the full implications of setting the design variables could be understood for complex systems and therefore unlikely that the design parameters can be manually selected to yield optimal system safety performance. An approach using fault tree analysis to predict the system availability of each system design has been used in conjunction with the grid-sampling method to find the optimal design [5]. Improvements in this approach have been made using binary decision diagrams [6–10], and also by incorporation

of a genetic algorithm [11, 12] to perform the optimization. This optimization technique allows a number of design alternatives to be investigated simultaneously. In using these search-based optimization techniques, the outcome is heavily reliant on the start point of the search.

An alternative to the traditional ad hoc approach to engineering design is statistically designed experiments (SDEs), which are a structured method to investigate the best settings for a potentially large number of decision variables [13, 14]. Statistical design of experiments means making many purposeful design changes at once and conducting several tests and evaluations before decisions are taken as to what the next steps in the development process should be. In this paper, the experimental design concepts are being used to try to gain a good starting point for the optimization. The better the starting point, the more efficient the optimization will be. In this way it is hoped to achieve about 80 per cent of the work required to reach an optimal design using about 20 per cent of the effort. The research shows, by means of application to a safety system, that adopting this approach can lead to generating an optimal design in a much more efficient manner than when applying traditional design processes. In addition, the technique can be used to search out good starting points, which can be used by more sophisticated optimization techniques to find the best system configuration.

2 STATISTICALLY DESIGNED EXPERIMENTS

2.1 Components of an SDE

In an SDE the variables to be changed are called *factors*. Prior to conducting an SDE (otherwise known as a factorial experiment), all factors must be identified and the possible values of each factor determined. These possible values are termed *levels*. The performance of the engineering system is characterized by a measurement of some aspect or function termed the *response*.

Purposeful design changes are determined using special matrices called *orthogonal arrays*. Consider, for example, a particular system consisting of three parameters: number of valves (A), valve type (B) and number of pressure transmitters (C). As regards each parameter, two settings are chosen to cover the range of interest. These factor levels define the experimental region and are listed in Table 1.

Table 1 Factor levels defining the experimental region

Factor	Levels	
	1	2
A: Number of valves	2	3
B: Valve type	1	2
C: Number of PTs	4	5

The goal is to minimize system unavailability, and, as such, the response is the probability of system failure, Q_{SYS} . The matrix experiment to define the experimental plan is stated in Table 2. It consists of four individual experiment designs corresponding to the four rows. The three columns of the matrix represent the three factors whose values are indicated in Table 1. Thus, the first design consists of two valves of type 1 and four pressure transmitters. The matrix experiment is the standard orthogonal array L_4 [15]. For any pair of columns, all combinations of factor levels occur, and they occur an equal number of times. This is called the *balancing property* and it implies orthogonality. This balancing property inherent in orthogonal arrays enables the identification of which design changes make the difference to the performance of a design.

A matrix experiment consisting of all possible combinations of the factors is termed 'full factorial'. The run size for a two-level full factorial design in k factors is 2^k , which quickly becomes prohibitive for a moderate amount of factors. The problem is exacerbated for factors with more than two levels. A subset or fraction of the full factorial design (a fractional factorial) tends to be used unless there are only a few potentially important factors to be studied. In the example above, the orthogonal array represents a 'one-half fraction' of the 2^3 design.

2.2 Steps in a statistically designed experiment

An outline of the statistically designed experimental procedure is as follows:

1. Definition of the aim of the experimental plan and selection of the response variable.
2. Selection of the factors that will be changed and the levels that will be used.
3. Choice of a matrix experiment such that the plan has a systematic and balanced pattern.
4. Analysis of the data from the matrix experiment to determine the effects of the various factors. The effects of the various factors can be determined by computing simple averages. The estimates of the factor effects are then used to determine the optimum factor settings.
5. Summary of the results in a response table and effects plot. The use of engineering knowledge and common sense is essential in interpreting the results.
6. Validation of conclusions from the experiment using follow-up runs and confirmation testing.

Table 2 Experimental plan— $L_4(2^3)$ orthogonal array

Experiment number	Columns			Q_{SYS}
	1	2	3	
1	1	1	1	0.2
2	1	2	2	0.4
3	2	1	2	0.3
4	2	2	1	0.2

3 SAFETY SYSTEM DESIGN EXAMPLE

The high-integrity protection system (HIPS) has been used previously to demonstrate design optimization using genetic algorithms [11, 12]. The full design considerations are outlined within these papers, along with the binary decision diagram technique, which is used to assess the availability of each design. The basic features of the system are shown in Fig. 1.

Its function 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 first level of protection is the emergency shutdown (ESD) subsystem. Pressure in the pipeline is monitored using pressure transmitters (PTs). 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. 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:

1. How many ESD valves are required (0, 1, 2)? E
2. How many HIPS valves are required (1, 2)? H
3. How many pressure transmitters for each subsystem (1, 2, 3, 4)? $N1, N2$
4. How many transmitters are required to trip? $K1, K2$
5. Which of two possible ESD/HIPS valves to select? V
6. Which of two possible pressure transmitters to select? P
7. Maintenance test interval for each subsystem (1 week–2 years)? $\theta1, \theta2$

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

To assess the performance of a potential system design, the system unavailability needs to be considered along with the

Fig. 1 High-integrity protection system

Table 3 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 unit	1×10^{-5}	36.0	1×10^{-5}	36.0	20	1

limitations that are placed on the system. Thus, the performance depends on four parts:

- (a) the probability of system failure (unavailability, Q_{SYS});
- (b) a penalty for the design exceeding the total cost constraint, C_{pen} ;
- (c) a penalty for exceeding the total maintenance downtime constraint, MDT_{pen} ;
- (d) a penalty for exceeding the spurious trip constraint, ST_{pen} .

These are combined to give a sole value to represent system performance for each design, referred to as the penalized system unavailability of the design. Calculating the penalized system unavailability, Q'_{SYS} , involves the derivation of the penalty formula for excess cost, maintenance downtime and spurious trip occurrences [11]. If a particular design exceeds any of the stated limits, the respective penalty is added to the system unavailability of the design in question

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

Q_{SYS} is calculated from the binary design diagram representation of the system fault tree using component failure and repair data given in Table 3.

4 APPLICATION OF THE STATISTICALLY DESIGNED EXPERIMENT TO OPTIMIZE THE HIPS

4.1 Aim and response variable

The means by which the performance of a safety system design is assessed (i.e. the response variable) is chosen to be the penalized system unavailability, Q'_{SYS} . The primary goal is to determine the optimal level of each design variable such that Q'_{SYS} is minimized. The secondary goal, which is addressed throughout the experimental procedure, is to determine the effect (or lack of effect) that each design variable has on Q_{SYS} , maintenance downtime, cost and the spurious trip frequency. The SDE is essentially a global optimization procedure that initially encompasses a large proportion of the entire search space. Attainment of the global minimum, i.e. the primary goal, with this somewhat crude approach is unexpected. However, it is expected, through attention to the latter goal, to determine promising areas in the search space and hence a starting point, or points, from which to commence a more sophisticated approach.

4.2 Choice of factors and levels

All ten parameters associated with the HIPS were included to perform the initial experiment. The intention was to screen out the less important factors before carrying out a more detailed follow-up experiment. Levels of the factors should be chosen to be sufficiently far apart to cover a wide experimental region. This makes it possible to identify good and bad regions of the search space. During subsequent refinement, experiment levels closer to one another can be chosen. Each factor and their alternate levels selected for consideration are listed in Table 4.

Table 4 Factors and associated levels

Factor	Levels		
	1	2	3
E	0	1	2
$K1$	1	2	
$N1$	2	3	4
H	1	2	
$K2$	1	2	
$N2$	2	3	4
V	1	2	
P	1	2	
$\theta 1$	30	40	50
$\theta 2$	30	40	50

4.3 Matrix experiment

An efficient way to study the effects of several factors simultaneously is to plan a matrix experiment using an orthogonal array. An orthogonal array is constructed from the knowledge of the number of factors, their levels and the desire to study interactions. In this initial experiment there are five two-level factors and five three-level factors. For the purpose of the screening experiment it was decided not to study specific interactions. Using the standard methods of constructing orthogonal arrays, the standard array $L_{27}(3^{13})$ was selected for the matrix experiment. References [16] and [17] provide further detail on array construction and standard arrays. The standard array has 13 columns and 27 rows. Each row has three distinct entries, namely 1, 2 and 3 (i.e. each column is a three-level column). As such, a three-level factor can be assigned directly to any column. Five of the chosen factors have two levels. The dummy level technique was used to assign each two-level factor to a three-level factor. The dummy level technique works on the basis that, if a factor A has two levels A_1 and A_2 , it can be assigned to a three-level column by creating a dummy level A_3 , which could be taken to be the same as either A_1 or A_2 . For a more detailed explanation, refer to reference [18].

The modified $L_{27}(2^5 3^8)$ array representing the 27 safety system designs to be investigated is translated using the level definition in Table 4 to create a clear experimental plan (see Table 5). Each design, dictated by the matrix experiment, was analysed using equation (1). The final column of Table 5 gives the resulting penalized unavailability of the specified system design.

4.4 Data analysis

Data analysis is concerned with estimating the effect of each parameter on the penalized system unavailability over the 27 designs investigated. The overall mean value of Q'_{SYS} for the experimental region was 0.0342. The effect of a factor is defined to be the change in the response produced by a change in the level of the factor. This is commonly termed the *main effect*. For example, the main effect of the valve type parameter at level 1, V_1 , is given by

$$m_{V_1} = \frac{1}{18} \sum_{i=1}^{18} Q'_{iSYS} = 0.0299$$

Table 5 Clear experimental plan

Design	<i>V</i>	<i>P</i>	<i>E</i>	<i>K1</i>	<i>N1</i>	<i>H</i>	<i>K2</i>	<i>N2</i>	θ_1	θ_2	Q'_{SYS}
1	1	1	0	1	2	1	1	2	30	30	1.4e-3
2	1	1	0	1	3	1	2	3	40	40	2.51e-3
3	1	1	0	1	4	2	2	4	50	50	2.07e-3
4	1	1	1	2	2	1	1	3	40	40	2.98e-3
5	1	1	1	2	3	1	2	4	50	50	3.59e-3
6	1	1	1	2	4	2	2	2	30	30	7.46e-3
7	1	2	2	2	2	1	1	4	50	50	0.1104
8	1	2	2	2	3	1	2	2	30	30	9.67e-3
9	1	2	2	2	4	2	2	3	40	40	0.109
10	1	1	1	2	2	1	2	2	40	50	4.2e-3
11	1	1	1	2	3	1	1	3	50	30	3.11e-3
12	1	1	1	2	4	2	2	4	30	40	2.97e-3
13	1	1	2	1	2	1	2	3	50	30	2.91e-3
14	1	1	2	1	3	1	1	4	30	40	0.0217
15	1	1	2	1	4	2	2	2	40	50	5.19e-3
16	1	2	0	2	2	1	2	4	30	40	0.0442
17	1	2	0	2	3	1	1	2	40	50	0.1017
18	1	2	0	2	4	2	2	3	50	30	0.1024
19	2	1	2	2	2	1	2	2	50	40	4.36e-3
20	2	1	2	2	3	1	2	3	30	50	4.32e-3
21	2	1	2	2	4	2	1	4	40	30	0.0573
22	2	1	0	2	2	1	2	3	30	50	1.6e-3
23	2	1	0	2	3	1	2	4	40	30	2.31e-3
24	2	1	0	2	4	2	1	2	50	40	3.87e-3
25	2	2	1	1	2	1	2	3	40	30	0.1025
26	2	2	1	1	3	1	2	2	50	40	0.1054
27	2	2	1	1	4	2	1	4	30	50	0.1026

where m_{V_1} denotes the main effect of parameter *V* at level 1, and Q'_{iSYS} denotes the penalized system unavailability for design *i*.

The main effect of each factor at each of its levels is specified in Table 6. A better feel for the relative effect of the different factors can be obtained using the analysis of variance (ANOVA) technique. The sum of squares due to factor *V*, SS_V , is equal to the total squared deviation of each level of *V* from the overall mean, *m*. Eighteen designs are investigated with *V* at level 1, and nine designs with *V* at level 2. Thus

$$SS_V = 18(m_{V_1} - m)^2 + 9(m_{V_2} - m)^2 \\ = 9.8 \times 10^{-4}$$

The sum of squares due to each factor can be seen in Table 6. This table indicates that the parameter *P* governing the pressure transmitter type contributes a major proportion of

the total variation in Q'_{SYS} . In fact, it is responsible for 83.1 per cent of the variation.

4.5 Selecting optimum factor levels

The primary goal in conducting the matrix experiment is to determine the best or optimum level for each factor. As regards the HIPS, the optimum level for each factor is the level that gives the lowest value of Q'_{SYS} in the experimental region. The estimated main effects can be used for this purpose. Therefore, the settings V_1 , P_1 , E_1 , $K1_2$, $N1_2$, H_1 , $K2_2$, $N2_1$, θ_1 , θ_2 would give the lowest penalized system unavailability. Note that the subscript denotes the level of that parameter.

The predicted best settings need not correspond to one of the rows in the matrix experiment (Table 5), as is the case here. Prior to implementing any design suggested by the technique, it must be fully evaluated. The confirmed

Table 6 Main effects

Factor	Main effect			Sum of squares (ANOVA)	% ANOVA
	Level 1	Level 2	Level 3		
<i>V</i>	0.0299	0.0427		9.8e-4	2.1
<i>P</i>	4.43e-3	0.0876		0.0386	83.1
<i>E</i>	0.0291	0.0372	0.0361	3.5e-4	0.75
<i>K1</i>	0.0385	0.032		2.5e-4	0.5
<i>N1</i>	0.0305	0.0282	0.0437	1.3e-3	2.7
<i>H</i>	0.0316	0.0394		3.6e-4	0.8
<i>K2</i>	0.045	0.0287		1.6e-3	3.4
<i>N2</i>	0.027	0.0369	0.0385	7.0e-4	1.5
θ_1	0.0218	0.0431	0.0376	2.2e-3	4.8
θ_2	0.0321	0.0331	0.0373	1.4e-4	0.3

performance characteristics associated with the estimated optimal design are a MDT of 112.7 h, a cost of 652 units, a spurious trip frequency of 0.28/year, a system unavailability of 0.0016 and therefore a penalized system unavailability of 0.0016.

The value of Q'_{SYS} realized for the predicted best settings is not as good as the best among the rows of the matrix experiment. The cause of this could be the coarse nature of the approach, or it may indicate the presence of significant interactions among the variables. Realization that the design proposed does not meet the desired optimal target means that practical implementation is not carried out and additional analysis and investigation are needed to find better settings.

4.6 Additional analysis

The main effects of the factors are their independent effects. If the effect of a factor depends on the level of another, then the two factors are said to have an interaction. Within engineering applications this interaction is commonplace. For example, if there is redundancy within the system in the form of a two out of three voting set-up, changing the level of redundancy has a direct effect on the number of components required to trip the system. For the HIPS, the large effect of parameter P dominates the effect of the other parameters. The variables in the trip mechanism, such as the number of pressure transmitters, the number required to trip and the type of pressure transmitter, are likely to have related effects. The main effects (shown diagrammatically in Fig. 2) clearly indicate that pressure transmitter type 1 is the optimum level for this factor.

As such, the main effects of $K1$, $N1$, $K2$ and $N2$ are revised using only a subset of the designs in the L_{27} array. That is, those designs with P set at level 1. The main effects (penalized system unavailability) for each of these variables for P at level 1 are specified in Table 7.

It can be seen that the optimal settings for $K1$, $N1$, $K2$ and $N2$ at $P1$ are levels 1, 1, 2 and 2 respectively. This gives a

Table 7 Main effects with P at level 1

Factor	Main effect for P at level 1		
	Level 1	Level 2	Level 3
$K1$	0.00596	0.0081725	
$N1$	0.002908	0.0062567	0.0131433
$K2$	0.01506	0.0036225	
$N2$	0.00443	0.0038517	0.010188

design specified by a one from two trip configuration for subsystem 1 and a two from three trip configuration for subsystem 2. A confirmation run of the revised prediction specifying the best design gives a MDT of 112.7 h, a cost of 652 units, a spurious trip frequency of 0.54/year and a probability of system unavailability of 0.0014 (no penalties incurred). It is an improvement over the initial prediction and equals the best in the original experiments table, i.e. as shown by design 1 of Table 8.

4.7 Considerations for follow-up experiment

To carry out a follow-up experiment, it must be determined which factors besides P have a strong effect on the response. It was noted that the main effects of each parameter were biased by significantly large values of Q'_{SYS} , which resulted from the exertion of penalties due to constraint violations. To investigate this further, the effect of each parameter on system cost, MDT and spurious trip frequency, F'_{SYS} , was established.

The main effect of each factor level with respect to system cost is shown in Table 9, as well as the sum of squares due to each factor and the percentage of variation for which the factor is responsible. These figures were also calculated for MDT (Table 10) and spurious trip frequency (Table 11). Factor E was found to explain a major proportion of the total variation in cost, 87 per cent, with H being the next largest contributor at 6 per cent.

Fig. 2 Plot of the main effect of each factor

Table 8 Fitness data for each design, plus averages

Design	1	2	3	4	5	6	7	8	9	
Cost	632	672	982	922	962	1212	1152	1142	1432	
MDT	110.9	85.8	91.5	110.5	90.5	183.7	116.5	190.7	174.2	
F_{SYS}	0.803	0.673	0.813	0.681	0.29	0.56	2.45	0.555	1.53	
Q_{SYS}	1.4e−3	2.51e−3	2.07e−3	2.98e−3	3.59e−3	8.6e−4	8.28e−3	2.25e−3	1.25e−3	
Q'_{SYS}	1.4e−3	2.51e−3	2.07e−3	2.98e−3	3.59e−3	7.46e−3	0.1104	9.67e−3	0.109	
	10	11	12	13	14	15	16	17	18	
Cost	902	1212	982	1172	1502	1212	612	872	622	
MDT	102.7	142.1	140.8	126.2	199.8	131.3	111.4	104.8	97.1	
F_{SYS}	0.289	0.690	0.552	0.298	1.22	0.828	1.183	1.515	1.51	
Q_{SYS}	4.2e−3	1.12e−3	1.74e−3	2.91e−3	8.98e−3	3.25e−3	4.19e−3	1.73e−3	2.45e−3	
Q'_{SYS}	4.2e−3	3.11e−3	2.97e−3	2.91e−3	0.0217	5.19e−3	0.0442	0.1017	0.1024	
	19	20	21	22	23	24	25	26	27	Average
Cost	1242	1062	1102	822	642	622	1002	772	792	972.4
MDT	117.3	142.2	130.4	105	90.1	68.6	143.9	88.9	129	123.2
F_{SYS}	0.638	0.547	1.33	0.455	0.364	0.886	1.96	1.56	3.66	1.03
Q_{SYS}	4.1e−3	2.29e−3	2.13e−3	1.6e−3	2.31e−3	3.87e−3	9.35e−3	5.36e−3	2.62e−3	0.003
Q'_{SYS}	4.36e−3	4.32e−3	0.0573	1.6e−3	2.31e−3	3.87e−3	0.1025	0.1054	0.1026	0.0342

Table 9 Main effects and variance of each factor with respect to cost

Factor	Main effect with respect to cost			Sum of squares	%ANOVA
	Level 1	Level 2	Level 3		
V	1010.8	895.4		79903	6.1
P	992	933.1		20815	1.6
E	719.8	973.1	1224.2	1144894	86.9
$K1$	970.9	923.4		43238	3.3
$N1$	939.8	982	995.3	15114	1.1
H	960.9	995.3		7100	0.5
$K2$	978.7	969.2		542	0.04
$N2$	956.4	990.9	969.8	5445	0.4
$\theta1$	973.1	973.1	970.9	29	0.002
$\theta2$	970.9	973.1	973.1	29	0.002

Variables E , $\theta1$ and H were calculated to account for a large proportion of the total variation in MDT. To a lesser extent, V was also found to contribute to the variation in MDT.

The parameters that contribute to the variation in spurious trip frequency were found to be those associated with the

Table 10 Main effects and variance of each factor with respect to MDT

Factor	Main effect with respect to MDT			Sum of squares	% ANOVA
	Level 1	Level 2	Level 3		
V	128.3	112.9		1432.2	5.2
P	123.6	249.9		373.5	1.3
E	96.14	125.8	147.7	12052.3	43.7
$K1$	123	123.3		0.4	0.001
$N1$	116	126.2	127.4	707.1	2.6
H	114.7	140.2		3919.9	14.2
$K2$	123.6	123		2.2	0.008
$N2$	122.1	123.7	123.9	17	0.06
$\theta1$	146	119.3	104.2	8064.4	29.2
$\theta2$	123.9	121.9	112.7	1011.9	3.7

Table 11 Main effects and variance of each factor with respect to F_{SYS}

Factor	Main effect with respect to F'_{SYS}			Sum of squares	%ANOVA
	Level 1	Level 2	Level 3		
V	0.91	1.23		0.62	4.5
P	0.66	1.77		7.4	53.3
E	0.91	1.14	1.04	0.24	1.7
$K1$	1.31	0.89		1.06	7.6
$N1$	0.97	0.82	1.3	1.07	7.7
H	1.04	1.02		2.7e-3	0.02
$K2$	1.5	0.81		2.6	18.7
$N2$	0.85	1.11	1.13	0.44	3.2
$\theta1$	1.06	1.02	1.01	0.13	0.09
$\theta2$	0.9	0.99	1.2	0.43	3.1

pressure transmitters. However, the parameter governing the pressure transmitter type accounted for over 50 per cent of the variation alone. A design that constitutes pressure transmitters of type 2 generally has a high spurious trip frequency and hence receives a substantial penalty. This explains the dominance of parameter P regarding variation in the penalized system unavailability. Significant variation in the trip frequency still exists in many of the parameters when only those designs in the matrix with pressure transmitter type 1 are considered. However, this variation occurs below the spurious trip limit (i.e. 1.0). Owing to their influence on the constraints of the safety system design, it was decided to carry out a follow-up experiment addressing parameters E , H , V , $\theta2$ and $\theta1$ specifically.

5 FOLLOW-UP EXPERIMENT

A follow-up experiment involving fewer factors was used to explore the response-factor relationship in more detail. The purpose of this step is to verify that the optimum conditions

suggested by the initial matrix experiment are indeed accurate and determine whether improvements can be made. It is possible that the verification experiment may identify strong interactions between parameters and highlight potentially misleading information. The factors selected for the follow-up experiment and their alternative levels are given in Table 12.

Observations from the screening experiment implied that the inclusion of three ESD valves is not beneficial, and the variable is now only set at two levels. The remaining variables were set to pressure transmitter type 1 with a trip configuration of one from two and two from three pressure transmitters for the ESD subsystem and HIPS subsystem respectively. These parameter values are the best settings predicted in the screening experiment.

In this study it was decided not only to estimate the main effects of the five factors listed in Table 12, but also to estimate four potential interactions identified from engineering experience. The four interactions considered to be most important were:

- (a) valve type and ESD valve number, $V \times E$;
- (b) valve type and HIPS valve number, $V \times H$;
- (c) ESD valve number and HIPS valve number, $E \times H$;
- (d) test interval 1 and test interval 2, $\theta_1 \times \theta_2$.

The matrix experiment to take account of the five factors and the four interactions is given in Table 13 (see reference [16] for details of experimental design construction). The values of the levels of each factor are given in the table as opposed to using their level code. This gives a clearer

indication of the design characteristics being investigated in each run.

The average values for system unavailability, cost, MDT, spurious trip frequency, system unavailability and penalized system unavailability for all designs are 1.26×10^{-3} , 855.1 units, 132 h, 0.63/year and 2.6×10^{-3} respectively. The best design is represented in column 24 of Table 13 and has a system unavailability of 7.36×10^{-4} (cost = 822 units, MDT = 130 h, spurious trip frequency = 0.72/year).

5.1 Data analysis

As with the first experiment, the main effect of each factor with respect to the penalized system unavailability was calculated and is shown in Table 14 and the effects plot in (Fig. 3). It was estimated from the main effects that the settings V_2 , E_1 , H_1 , θ_{14} and θ_{24} would give the lowest penalized system unavailability, where the subscript number identifies the factor level. A confirmation run gives MDT = 78 h, cost = 602 units, spurious trip frequency = 0.625 per year and probability of system unavailability = 0.0031 (no penalties incurred). This design is poor compared with the best design from the follow-up experiment, the unavailability of which is considerably less at 7.36×10^{-4} . Also, the cost of this design is only 622 units, indicating the possibility of utilizing further resources. Therefore, consideration is given to the key interactions.

Table 15 and Fig. 4 represent the data for the interactions $V \times E$ and $V \times H$. Specifically, the main effect of factor E is

Table 12 Factor levels in the follow-up experiment

Factor	Levels			
	1	2	3	4
V	1	2		
E	1	2		
H	0	1		
θ_1	25	30	35	40
θ_2	25	30	35	40

Table 14 Main effects of factors with respect to penalized system unavailability

Factor	Level			
	1	2	3	4
V	3.32e-3	1.46e-3		
E	1.93e-3	3.27e-3		
H	1.97e-3	3.22e-3		
θ_1	3.81e-3	2.59e-3	2.12e-3	1.87e-3
θ_2	3.37e-3	2.46e-3	2.32e-3	2.23e-3

Table 13 Matrix experiment

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
V	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
H	1	1	1	1	2	2	2	2	1	1	1	1	2	2	2	2
θ_1	25	25	30	30	35	35	40	40	35	35	40	40	25	25	30	30
θ_2	25	30	35	40	25	30	35	40	25	30	35	40	25	30	35	40
	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
V	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
E	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
H	1	1	1	1	2	2	2	2	1	1	1	1	2	1	2	2
θ_1	35	35	40	40	25	25	30	30	25	25	30	30	35	35	40	40
θ_2	35	40	25	30	35	40	25	30	35	40	25	30	35	40	25	30

Fig. 3 Main effects plot of factors in follow-up experiment

 Table 15 $V \times E$ and $V \times H$ interaction effects

V	E		H	
	1	2	1	2
1	3.65e-3	7.21e-3	1.83e-3	4.7e-3
2	1.75e-3	1.99e-3	1.3e-3	2.4e-3

 Table 16 $E \times H$ interaction data

H	E	
	1	2
1	1.92e-3	2.32e-3
2	1.54e-3	4.59e-3

calculated at the first level of factor V , then at the second level of factor V ; $V \times H$ is considered in a similar manner. The effects for $E \times H$ and $\theta_1 \times \theta_2$ are also given in Tables 16 and 17 and visually in Fig. 5.

If there is no interaction between two factors, an effects plot of one factor against both levels of the other will portray two parallel lines. No interaction implies that a change in level of one factor will produce the same change in the response regardless of the level of the other factor. In this case, the optimum levels identified by the main effects are valid. If the lines in the effects plot are not parallel but have the same direction of movement, then an interaction is present. However, the optimum levels identified in the main effects are likely still be to valid. This is termed a synergistic interaction. However, an inconsistent direction of movement on the effects plot implies a strong interaction between the factors. In such cases the optimum level

 Fig. 4 Effects plot for $V \times H$ and $V \times E$

identified by the main effects may be misleading. This is termed an antisynnergistic interaction.

It is apparent from the main effect and interaction plots that:

1. There is a synergistic interaction between the parameters V and E and V and H . The interaction is stronger in the former. The best settings for the parameters levels V , E and H are 2, 1 and 1 respectively (i.e. valve type 2 with no ESD valves and one HIPS valve).
2. There is an antisynnergistic interaction between parameters E and H . This makes sense as both incur significant cost to the design. The results from the interaction investigation contradict the main effects data which indicated that, when the number of ESD valves is 0 (its optimal setting), the best level for factor H is 2 (i.e. two HIPS valves fitted).
3. Strong interaction exists between the maintenance test interval parameters, and, as such, the main effects associated with θ_1 and θ_2 may be misleading. The implication from Fig. 5 is that the higher maintenance test interval values are generally beneficial. This is due to the fact that such values do not incur a penalty as a

 Table 17 $\theta_1 \times \theta_2$ interaction data

θ_1	θ_2			
	1	2	3	4
1	6.16e-3	5.12e-3	1.84e-3	2.16e-3
2	2.1e-3	1.17e-3	3.7e-3	3.4e-3
3	3.01e-3	1.78e-3	1.86e-3	1.85e-3
4	2.22e-3	1.77e-3	1.58e-3	1.81e-3

Fig. 5 Effects plot for the $E \times H$ and $\theta_1 \times \theta_2$ interactions

Table 18 Characteristics of the estimated optimal design

Subsystem 1	
E	0
$K1/N1$	1/2
θ	30
Subsystem 2	
H	2
$K2/N2$	2/3
θ	30
V	2
P	1
MDT	130
Cost	822
Spurious trip frequency	0.72
System unavailability	7.36×10^{-4}
Penalised system unavailability	7.36×10^{-4}

result of MDT violation. It is most likely that the fittest designs are associated with the lower test values, but such results are obscured by penalties due to MDT violation. Despite this, the best setting for both test parameters was predicted to be level 2 (i.e. 30 week intervals for each).

5.2 Optimum factor settings

The best settings of the factors suggested by the above results are identical to those of the best design in the design matrix of the follow-up experiment (note that the best settings of factors P , $K1$, $N1$, $K2$ and $N2$ are carried over from the initial experiment). As such, a verification experiment is not required to establish the response associated with the predicted best design. The performance characteristics of the resulting best design are given in Table 18. The safety system is over 99.9 per cent available and achieves full use of the MDT resource.

6 DISCUSSION OF RESULTS

Data analysis of the initial experiment clearly indicated that the optimal safety system design should constitute

pressure transmitters of type 1. It was further implied that the optimal trip configuration using this pressure transmitter is one from two for subsystem 1 and two from three for subsystem 2. It was noted that the penalized designs were causing a bias in the main effects, and, as such, further analysis was carried out to determine which parameters had the greatest effect on constraint violation. The implication was that parameters E , H , V and θ_1 are the most influential. Logic dictates that parameter θ_2 is also influential as regards system MDT.

In light of this evidence, a more detailed follow-up experiment was implemented using the factors stated above. A study of potential key interactions was also incorporated. It was found that parameters V and E and V and H portrayed a synergistic interaction, whereas E and H and both test parameters portrayed an antis synergistic interaction. The interaction plots indicated that the optimal safety system design incorporated no ESD valves and two HIPS valves, with both test intervals set at 30 week intervals. The optimum level predicted for each factor corresponded to the best design in the follow-up matrix experiment. The system unavailability of the design is 7.36×10^{-4} with no constraint violations.

7 APPLICATION OF LOCAL OPTIMIZATION TECHNIQUES

It is expected that $K1$ and $N1$, in addition to $K2$ and $N2$, will portray significant interaction. A matrix experiment could be developed in a similar vein to that described in section 5 to investigate these interactions further. In the main, however, the experimental approach is a global technique that considers the entire search space to glean greater knowledge in order to determine potentially good (and bad) areas of the space. This knowledge can then be used to assist further, more sophisticated techniques.

The grid-sampling technique [19] and logical search approach [19] are, in contrast, localized, hill-climbing methods that rely on a good start point to achieve an optimal solution. As opposed to further refinement of the resulting design specified in Table 18, using SDEs, the design vector is used as an initial design point in the aforementioned localized approaches.

Using the grid-sampling technique, it was found that a safety system design more optimal than the initial design vector could not be achieved. An explanation for this could be that the initial design vector is exceedingly fit. As such, the errors introduced via the use of approximate objective functions to analyze the search space about the initial design point are large in comparison with the difference between the initial design vector and the global minimum.

The final design resulting from application of the logical search approach has a one from two as opposed to a two from three pressure transmitter trip configuration constituting subsystem 2, in addition to modification of the maintenance test interval parameters. An improvement of $1.3 \times$

10^{-3} in system unavailability is achieved, resulting in a safety system design that is over 99.92 per cent available. The logical search approach implements an accurate investigation of the region directly surrounding the value of each variable in the initial design vector while considering the degree of interaction between the design variables. The initial point proves in this case to be sufficiently fit for the believed global optimum to be found.

8 CONCLUSIONS AND SUMMARY

The use of orthogonal arrays to develop an experimental design is an efficient way to study the effects of several control factors simultaneously. It is beneficial to adopt an iterative approach to acquire knowledge as the experimental plan progresses, and thus adapt the process accordingly. Designs suggested by the technique are tested for confirmation of their predictive potential, preventing the selection of a poor design. In the worst-case scenario (i.e. if any factors exhibit strong interactions), good and bad regions of the search space are identified and an indication of the relative importance of each factor is acquired. As such, further exploration can proceed using an appropriate local search technique based on the information established. In the best-case scenario, the optimum level for some, if not all, of the factors is determined. Importantly, the experimental effort required is much smaller when compared with other methods of exploration such as trial and error, one factor at a time and full factorial experiments.

It is recognized that investigating many design parameters at two relatively extreme values does not carry the sophistication of other more detailed and complex methods. However, the more detailed design methods work more efficiently if they are working to update a reasonable design. It is suggested that this SDE approach be used not to produce a final design itself but to locate a good starting point for a more complex design approach that is capable of modelling each design variable at more levels.

ACKNOWLEDGEMENT

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

REFERENCES

- 1 **Andrews, J. D.** and **Moss, T. R.** *Reliability and Risk Assessment*, 2nd edition, 2002 (IMechE, London).
- 2 **Billinton, R.** and **Allan, R.** *Reliability Evaluation of Engineering Systems*, 2nd edition, 1993 (Pitman, New York).
- 3 **Villemeur, A.** *Reliability, Maintainability and Safety Assessment*, 1992, Vol. 2 (Wiley, Chichester).
- 4 **Henley, E. J.** and **Kumamota, H.** *Reliability Engineering and Risk Assessment*, 1981 (Prentice-Hall, Englewood Cliffs, NJ).
- 5 **Andrews, J. D.** Optimal safety system design using fault tree analysis. *Proc. Instn Mech. Engrs, Part E: J. Process Mechanical Engineering*, 1994, **208**, 123–131.
- 6 **Rauzy, A.** New algorithms for fault tree analysis. *Reliability Engng and Syst. Safety*, 1993, **40**, 203–211.
- 7 **Sinnamon, R. M.** and **Andrews, J. D.** Fault tree analysis and binary decision diagrams. In Proceedings of 1996 Reliability and Maintainability Symposium, Las Vegas, January 1996, pp. 215–222.
- 8 **Sinnamon, R. M.** and **Andrews, J. D.** New approaches to evaluating fault trees. In Proceedings of ESREL 95 Conference, June 1995, pp. 241–254.
- 9 **Sinnamon, R. M.** and **Andrews, J. D.** Improved efficiency in qualitative fault tree analysis. *Qual. and Reliability Engng Int.*, 1997, **13**, 285–292.
- 10 **Sinnamon, R. M.** and **Andrews, J. D.** Improved accuracy in quantitative fault tree analysis. *Qual. Reliability Engng Int.*, 1997, **13**, 293–298.
- 11 **Andrews, J. D.** and **Pattison, R. L.** Optimal safety system performance. In Proceedings of the Annual Reliability and Maintainability Symposium, Philadelphia, 13–16 January 1997, pp. 76–84.
- 12 **Pattison, R. L.** and **Andrews, J. D.** Genetic algorithms in optimal safety system design. *Proc. Instn Mech. Engrs Part E: J. Process Mechanical Engineering*, 1999, **213**(E3), 187–197.
- 13 **Box, G.** and **Draper, N. R.** *Empirical Model-Building and Response Surfaces*, 1997 (John Wiley, New York).
- 14 **Grove, D. M.** and **Davies, T. P.** *Engineering Quality and Experimental Design*, 1992 (Longman Scientific and Technical, Harlow).
- 15 **Plackett, R. L.** and **Burman, J. P.** The design of optimal multifactorial experiments. *Biometrika*, 1956, **33**, 305–325.
- 16 **Lin, D. K. J.** Making full use of Taguchi's orthogonal arrays. *Qual. and Reliability Engng Int.*, 1994, **10**, 117–121.
- 17 **Montgomery, D. C.** *Design and Analysis of Experiments*, 3rd edition, 1991 (John Wiley, New York).
- 18 **Misra, K. B.** and **Sharma, U.** An efficient algorithm to solve integer programming problems arising in system reliability design. *IEEE Trans. Reliability*, 1991, **40**(1), 81–91.
- 19 **Pattison, R. L.** Safety system design optimisation. PhD thesis, Loughborough University Library, 1999.