An offshore safety system optimization using a SPEA2 based approach

PUBLISHER

© IMechE / Professional Engineering Publishing

REPOSITORY RECORD

Riauke, Jelena, and L.M. Bartlett. 2008. “An Offshore Safety System Optimization Using a SPEA2 Based Approach”. figshare. https://hdl.handle.net/2134/3937.

An Offshore Safety System Optimization using a SPEA2 based Approach

J Riauke and **L M Bartlett**

Department of Aeronautical and Automotive Engineering, Loughborough University, Loughborough, LE11 3TU. UK. Email addresses : J.Riauke@yahoo.co.uk, L.M.Bartlett@lboro.ac.uk.

Abstract

A safety system is an essential part of any industrial system as it operates to prevent the occurrence of certain conditions and their future development into a hazardous situation. Failure of such systems may have catastrophic consequences from small injuries to even death of members of the workforce and public, therefore, it is imperative to minimize safety system unavailability and also find the balance between its unavailability and other limitations on its operation, for example, life cycle cost and spurious trip frequency. Hence, a multi-objective optimization of the system design is required. This paper describes a design optimization scheme using multi-objective genetic algorithms (MOGAs) applied to a firewater deluge system (FDS) on an offshore platform, which works to supply on demand water and foam at a controlled pressure to a specific area on the platform, protected by the deluge system.

Keywords: safety systems, unavailability, optimization, genetic algorithms, SPEA2

1 INTRODUCTION

The system design can be chosen by traditional approaches, which combine the preliminary design, analysis, appraisal and redesign stages until what is regarded as an acceptable design is achieved. To find an optimal design a process is required which considers a number of design variables. Genetic algorithms (GAs) are a group of techniques which allow this type of parallel processing [1]. Previously the firewater deluge system unavailability has been optimized by the simple genetic algorithm [2]. However, it is not the only important criterion of the large safety system (for example, system cost, spurious trip frequency) and, hence, multi-objective system optimization should be utilized. There are a number of different techniques that can be used to carry out such optimization problems, for example, simulated annealing, tabu search, and genetic algorithms. A comparison of the strengths and weaknesses of these techniques is given in references [3, 4]. The Improved Strength Pareto Evolutionary Algorithm (SPEA2) is chosen to perform the FDS optimization [5]. This is a relatively recent and effective multi-objective genetic algorithm (MOGA) technique, which incorporates a fine-grained fitness assignment strategy, a density estimation technique and an enhanced archive truncation method.

During the last few years SPEA2 has been successfully applied to safety system optimum design. In 2003 Greiner [6] applied different multi-objective evolutionary algorithms (SPEA2, NSGSII and controlled elitist-NSGAII) to a Containment Spray Injection System of a nuclear power plant. In 2004 Hiroyasu [7] optimized heavy-duty diesel engines by a hybrid of SPEA2 and NSGAII techniques. In 2007 Martorell [8] applied SPEA2 based MOGA to the high pressure injection system (HPIS) of a nuclear power plant optimization. The optimization criteria involved system unavailability and cost. In 2007 Aribia [9] found optimal reactive dispatch in terms of three objectives (compensational device cost, transmission losses and the voltage deviation) by SPEA2 based optimization tool.

Analysis of individual system designs of the FDS are carried out using the fault tree method [10] and the binary decision diagram approach [11]. The optimization criteria involves system unavailability, cost and spurious trip frequency. Comparison of the results produced by the implemented SPEA2 technique to those obtained by using the simple genetic algorithm is carried out, yielding results, that indicate that the technique is suitable for application in this industrial domain.

2 OPTIMIZATION TECHNIQUE

The developed optimization technique combines the advantages of fault tree analysis (FT) for system failure logic representation, binary decision diagrams (BDD) for system design quantification and the Improved Strength Pareto Evolutionary Algorithm (SPEA2) for system design optimization. The main features of FT and BDD techniques are discussed briefly in section 2.1. Section 2.2 describes the SPEA2 method.

2.1 FT Analysis and BDD

Fault tree analysis is a deductive (top-down) technique, structured in terms of events rather than components [10]. It acts as a visual tool, a graphical representation of the various parallel and sequential combinations of faults that lead to the occurrence of the top event. Hence, the fault tree have been chosen to represent the safety system failure logic.

The FT can be constructed for each potential system design, however it is an impractical task when there are a large number of design options. This problem can be solved by including house events in the FT structure. House events are used to model two state events which either occur or do not occur, and, therefore, have probabilities 1 or 0. They provide a very effective means of turning sections of the fault tree on and off. One of the advantages of this is that the same fault tree can be used to model several scenarios.

The system unavailability and spurious trip frequency can be calculated directly from the FT for each potential design. However, often real safety systems require a large FT due to the number of components. In such cases analysis of the top event probability usually requires the use of approximations, since the exact technique makes significant use of computer recourses. For these situations the Binary Decision Diagram (BDD) approach is potentially the most successful [11]. It has been decided to use the BDD technique, since the method improves both the efficiency of determining the minimal cut sets of the fault tree and also the accuracy of the calculation procedure used to determine the top event parameters.

2.2 SPEA2 Algorithm

The developed optimization tool incorporates the SPEA2 method, designed by Zitzler, Laumanns and Thiele [5]. It is an improved version of the strength Pareto evolutionary algorithm (SPEA), developed by Zitzler and Thiele in 1998 [12]. SPEA2 is a relatively recent evolutionary technique for finding or approximating the optimal solution set for multiobjective optimization problems. It has shown very good performance in comparison to other multiobjective genetic algorithms [5]. The suggested algorithm can be explained in six steps:

Step 1. *Initialization*: Generate an initial population of potential designs and create the empty archive called external set. The resultant archive after the optimization is complete will hold the set of best designs.

Step 2. *Fitness assignment*: Calculate fitness value of each potential design in the initial population. This fitness value represents the suitability of the design given by the optimization criteria.

Step 3. *Environmental selection*: Copy all nondominated designs to the archive (given the optimization is a minimization problem, the nondominated solutions are those, which have at least one smallest optimization parameter value). If the archive is exceeded reduce it by means of the truncation operator, otherwise fill the archive with dominated designs from the initial population. The number of designs contained in the archive is to remain constant over time.

Step 4. *Termination*: If the maximum number of generations is reached or another stopping criterion is satisfied then the set of possible designs are those in the archive. Algorithm complete. Else continue to step 5.

Step 5**.** *Mating selection*: Perform binary tournament selection with replacement on the archive in order to fill the mating pool (group of designs upon which genetic modification may occur), i.e.:

a) Randomly (using uniformly distributed random numbers) select two individuals out of the archive.

b) Copy the one with the better (i.e. lower for the FDS optimization problem) fitness value to the mating pool.

c) If the mating pool is full, then stop, else go to step (a).

Step 6. *Variation*: Apply recombination and mutation operators to the mating pool and set the archive to the resulting population (recombination is a process in which individual strings are copied according to their fitness values, and mutation is an operation that provides a random element in the search process). Increment generation counter and go to *Step 2*.

3 FDS SYSTEM

The system whose design is to be investigated is a Firewater Deluge System (FDS), which is an essential part of an offshore platform and supplies, on demand, water and foam at a controlled pressure to a specific area, protected by a deluge system [2]. The main features of the deluge system are shown in figure 1. The FDS comprises a deluge skid, firewater pumps, with associated equipment and ringmains, and aqueous film-forming foam (AFFF) pumps, with associated equipment and ringmains. The description of the main parts of the FDS is provided in section 3.1. Section 3.2 represents the system design variables. The FDS failure events and data are discussed in section 3.3.

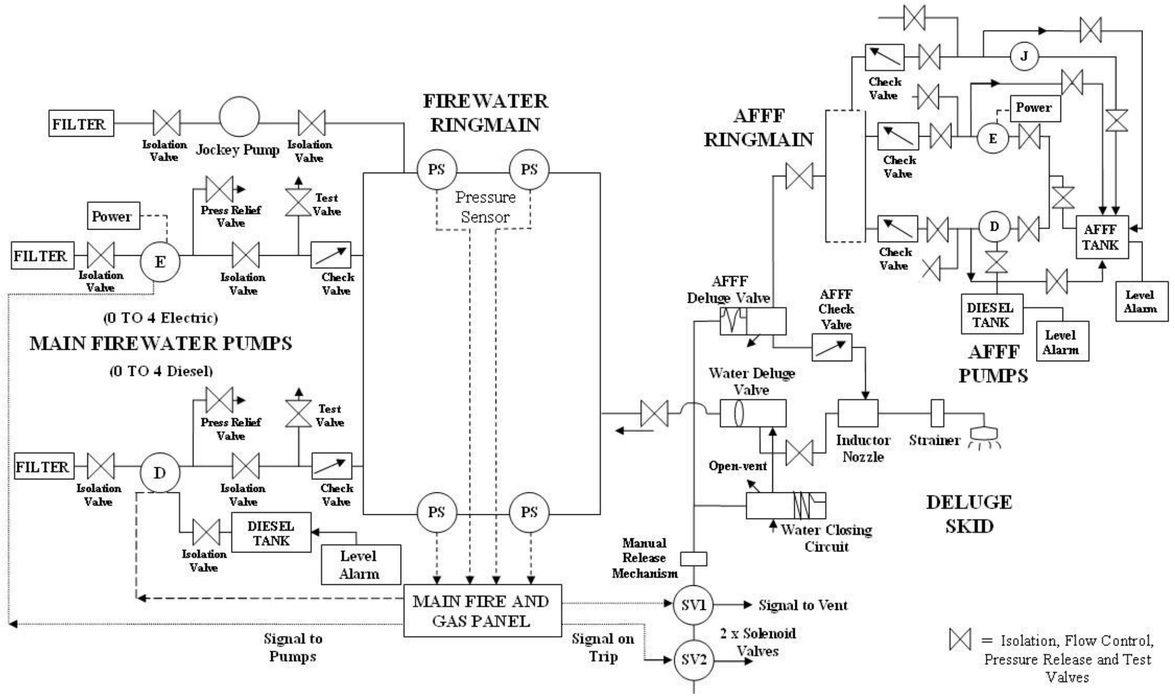


Fig. 1 Firewater deluge system

3.1 Main Parts of the FDS

There are three main parts of the FDS system:

The Deluge System: The deluge valve set with all associated equipment is mounted on a fabricated steel framework called a skid. Skids are situated on the processing platform where an incident can occur. In this situation the associated equipment acts to spray water onto the affected area. The three main elements of the deluge valve set are the main distribution line, a water closing circuit and a control air circuit.

The system can be operated either manually by opening the systems local manual release valve on the skid or automatically: the main fire and gas panel (MFGP) gives the signal to the solenoid valves to de-energize and open thus releasing air pressure from the control air circuit. After the pressure drop the valmatic release valve opens and the water from the water closing circuit runs to drain. This process results in the fall of pressure on the deluge valve diaphragm. When the pressure on the diaphragm has fallen sufficiently, the firewater main pressure, acting on the underside of the deluge valve clack, overcomes the load imposed by the diaphragm. This allows water to flow into the distribution pipes, through the nozzle and onto the hazard.

The deluge valve set is also fitted with an aqueous film-forming foam (AFFF) supply line. Instrument air pressure maintains the valmatic release valve and AFFF valve closed. The AFFF valve and valmatic release valve open simultaneously when the air pressure drops in the control air circuit. This reaction is caused by the de-energising of the solenoid valves. As the water flows through the foam inductor in the main distribution line, foam concentrate is induced from the AFFF line via the foam proportioner. As a result, the solution of water and approximately 3% foam then feed into the distribution network, through the nozzles and onto the hazard.

Firewater Supply and Distribution System: The deluge systems are connected to a pressurised ringmain network. The jockey pump maintains the ringmain pressure by drawing water from the sea. The pressure transducers detect the falling pressure and subsequently send the signal to the MFGP, which activates the firewater pumps to supply water direct from the sea at sufficient pressure to meet the deluge requirement. In inactive standby the pumps remain not needed. Both pumps can be started manually at the fire control panel. There are two sets of fire pumps: one set is powered from the main electric power plant and the other from their own dedicated diesel engines. The diesels have a day tank, which provides a 24 hour supply. The tank is fitted with a low level alarm, giving a signal in the central control room.

AFF Supply and Distribution System: The foam concentrate is stored in a stainless steel tank and is distributed through a stainless steel ringmain network. Similar to the firewater supply and distribution system, the tank has a low level alarm fitted, sounding in the central control room. The foam system is kept at approximately the same pressure as the firewater system by a continuously running air driven jockey pump. There are two types of AFFF pumps: one supplied from the platform power plant, the other are diesel driven. When any firewater pump starts to supply foam at sufficient pressure to meet design requirements, the AFFF pumps start automatically. It should be noted that the pumps not needed remain in standby. The diesel supply to the firewater diesel pumps is separate from that of the AFFF diesel pumps.

3.2 FDS Design Variables

The firewater deluge system is a relatively complicated system. Therefore, there are a huge number of design options which can be considered. The overall FDS system can be represented by the following 17 design variables with range specified in brackets:

- N – number of pressure transmitters on the ringmain (1, 2, 3, 4),
- K – number of pressure transmitters required to trip (1 - N),
- P – pressure transmitter type (1, 2, 3),
- F_E – number of electrically powered firewater pumps (0-4),
- F_D – number of diesel firewater pumps (0-4);
- F_P – the percentage capacity of the firewater pumps (100%, 50% or 33.33%),
- F_T – the pump type for 50% and 33.33% capacity pumps (1 or 2),
- A_E – number of the electrically powered AFFF pumps (0-2),
- A_D – Number of diesel AFFF pumps (0-2),
- A_P – the percentage of the capacity for the AFFF pumps (100% or 50%),
- W – water deluge valve type (1, 2 or 3),
- D – AFFF deluge valve type (1, 2 or 3),
- C – type of the materials for certain purpose (new or old),
- θ_P – maintenance test interval for the firewater and AFFF pump system (1-28 days),
- θ_R – maintenance test interval for the ringmain (1 to 24 weeks),
- θ_D – maintenance test interval for the deluge skid (3-18 months in 3 monthly interval only),
- θ_{PM} – preventative maintenance on components of wear-out type (3-18 months in 3 monthly intervals only).

It is important to notice that similar to the AFFF system pumps all pumps in the firewater system are to be of the same capacity. In addition, electric and diesel pumps of 100% capacity in the firewater system are of one type only, as are both 100% and 50% pumps in the AFFF system.

3.3 Failure Data

There are two main types of the FDS events. The type 'HE' states that the event is a human error. On the other hand, type 'CO' denotes that the event is a component failure. The 'wear-out' components are denoted by 'W'. In contrast, 'NW' states that the component is of 'non-wear-out' type. It is important to notice, that preventative maintenance is only carried out on components of wear-out type.

The system is checked for corrosion build-up. Consequently, corrosion resistant components are introduced, where 'n' and 'o' correspond to the non-corrosion resistant and corrosion resistant materials respectively.

Tables 1 – 3 show the subsets of the failure events and data for the deluge system, firewater supply and AFFF supply distribution systems respectively.

Table 1 Subset of failure events for deluge system

Event Name	Event Description	Event Type	Rates
WBN (new)	Deluge nozzle on the water spray system blocked, new type material.	CO	NW
WV1	Water deluge valve type 1 fails to open	CO	NW
MRM	Manual release mechanism fails to dump instrument air.	CO	NW
AIVC	Operator leaves the normally locked open butterfly valve on the AFFF distribution line in the shut position.	HE	-
AV1	AFFF deluge valve type 1 fails to open on demand	CO	NW

Table 2 Subset of failure events for firewater supply and distribution system

Event Name	Description	Event Type	Rates
ESF	Failure of electricity supply to electric driven firewater pumps.	CO	NW
DIVB	Diesel engine supply is blocked.	CO	NW
DIVC	Diesel supply is inadvertently left isolated after maintenance.	HE	-
E_100	Failure of electric pump with 100% capacity.	CO	W
E1_50	Failure of electric pump type 1 with 50% capacity.	CO	W

It is important to notice, that the electricity supply (ESF) is global to all electric pumps. In addition, a single diesel tank supplies all fitted firewater diesel pumps.

Table 3 Subset of failure events for AFFF supply and distribution system

Event Name	Description	Event Type	Rates
ATIVB	Normally locked open ball valve on AFFF tank outlet blocked.	CO	NW
ATIVC	AFFF supply left isolated after maintenance.	HE	-
AE_100	Failure of AFFF electric pump with 100% capacity.	CO	W
AD_100	Failure of AFFF diesel pump with 100% capacity.	CO	W

Failure and repair data, maintenance effort and costs are provided for all components. The human error events only require specification of the probability of occurrence.

The unavailability, $Q(t)$, for the majority of FDS components is calculated by using the standard scheduled maintenance formula (i.e., $\lambda\left(\frac{\theta}{2}+\tau\right)$). However, the pumps are of wear-out type, therefore, the Weibull distribution is used. This distribution is chosen because in contrast to the exponential distribution Weibull is able to model increasing and decreasing failure rates. Thus, lending itself to the first (wear-in) and last (wear-out) phases of the bathtub curve in addition to the useful life period. It is characterised by a hazard rate function of the form given in equation 1,

$$\lambda(t)=\frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1},\ \eta>0,\ \beta>0,\ t\geq 0, \tag{1}$$

where β is referred to as the shape parameter and η is the scale parameter (or characteristic life), which influences both the mean and spread of the distribution. Modifying the value of β has a dramatic effect on the probability density function $f(t)$ (Equation 2):

$$f(t) = \lambda(t)\exp\left(-\left(\frac{t}{\eta}\right)^{\beta}\right). \tag{2}$$

When $\beta < 1$, the hazard rate applies to the burn-in phase. On the other hand, for $\beta = 1$ the hazard rate is constant and the distribution is identical to the exponential. When $\beta > 1$, the hazard rate applies to the wear-out phase. For $\beta \geq 3$, the probability density function, $f(t)$, tends toward a normal distribution, thus portraying symmetry. β and η parameters are provided for all related system components.

Table 4 FDS Design Limitations

Limitation	Maximum Value (per year)
Total life cycle cost (*i.e. the sum of the initial cost and total cost of maintenance effort*)	< 125 000 units
Total cost of testing the system	< 20 500 units
Total cost of preventative maintenance effort	< 13 500 units
Total cost of maintenance effort (*i.e. the sum of the cost of corrective maintenance due to repair of dormant and spurious failure, total cost of testing the system and total cost of preventative maintenance*)	< 44 000 units
Acceptable number of times that a spurious system shutdown occurs	< 0.75 times

4 DESIGN LIMITATIONS

System unavailability is certainly the most important optimization criterion for this system, which is required to operate on demand. However, available resources are limited and, therefore, some restrictions have been placed on the potential FDS design. The summary of these limitations is shown in table 4.

5 FDS OPTIMIZATION

The C++ package was used to build the FDS optimization software called ISPEASSOP (Improved Strength Pareto Evolutionary Algorithm Safety System Optimization Procedure). The program consists of three main parts. The first part is responsible for the initial population initialization and evaluation of each potential design life cycle cost (section 5.1). The second part is responsible for FDS unavailability and spurious fault tree construction for each design, their conversion to binary decision diagrams and calculation of the FDS unavailability and spurious trip frequency (section 5.2). The final part of the program is an implemented SPEA2 algorithm for the FDS optimization (section 5.3).

5.1 ISPEASSOP Part 1

This part of the program concentrates on the generation of the initial population and life cycle cost evaluation for each potential system design.

Coding and initializing the population: The number of strings for the initial population for a problem is not defined, thus, based on the FDS optimization by simple GAs [2], initial research has used 20. Each potential system design is described by 17 parameters (section 3.2), where each parameter value is calculated according to the binary coding system.

Each parameter must be allocated a particular number of bits, in order to accommodate the largest possible value in binary form. For example, the parameters governing the maintenance test interval for the deluge skid and preventative maintenance on the components of wear-out type, θ_D and θ_{PM} respectively, require 6 bits (3 bits each) of the total string to accommodate the maximum time span of 18 months (in three monthly intervals). In total, each string representing all design variables is 43 bits in length. It can be interpreted as a set of concatenated integers in binary form, as shown in figure 2.

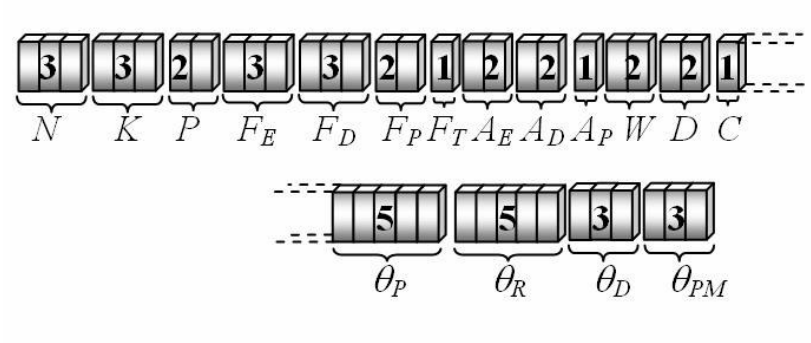


Fig. 2 Binary representation of the solution string

The restricted range of values assigned to each parameter does not in each case correspond to the representative binary range on the solution string. The total number of possible design options considering the allocated space for all 17 design variables is 8, 254, 927, 142, 912. However, only 56, 435, 097, 600 of these designs correspond to feasible solutions. For this reason a specialized procedure is used to code, to initialize and to check the feasibility of each string. In the initialization step infeasible strings are randomly regenerated.

Life Cycle Cost evaluation: The FDS life cycle cost is an important system optimization parameter due to the constraints imposed (Table 1). The important component of the life cycle cost is the initial cost to build the FDS (*SIC*). However, the system running costs must also be taken into account. These costs include only the maintenance activity, including the cost of corrective maintenance (*SCMC*) to repair any problem highlighted by system testing, the cost of preventative maintenance carried out at regular intervals on components that exhibit wear-out and the cost of system testing at regular intervals [2]. All these costs are evaluated over a period of 1 year.

Each component has an initial purchase cost and a storage cost. The storage cost depends on the number of spare items stored and the cost to store each item. The corrective maintenance cost of each component depends on the expected number of failures and the cost to repair each failure. Consider component *i*, the corrective maintenance of this component (CM_i) can be calculated as:

$$CM_i = \left(W_i^D + W_i^S\right)\left(C_R \cdot C_{HR} + C_{SR}\right), \qquad (3)$$

where W_i^D and W_i^S are the expected number of dormant and spurious failures for component *i* over the one year time period. C_R, C_{HR} and C_{SR} denote the number of hours of manual work required to test the component, the cost per hour of manual work to repair failure and the cost of spares for each repair carried out respectively.

The preventative maintenance is required only for the wear-out type components. The preventative maintenance cost per year of each component depends on the number of times preventative maintenance is carried out in the year and the cost per effort. The total FDS preventative maintenance cost (*SPMC*) is, therefore, calculated as the sum of the preventative maintenance costs (PMC_i) incurred by each component *i*. PMC_i is given by

$$PMC_i = \left(\frac{8760}{\theta_{PM}}\right)\left(\left(H_P \cdot C_{HP}\right) + C_{SP}\right), \qquad (4)$$

where θ_{PM} is converted to hours, H_P is the number of hours manual work required to carry out preventative maintenance, C_{HP} denotes the cost per hour of manual work to carry out preventative maintenance, and C_{SP} is the cost of spares each time preventative maintenance is undertaken.

System tests are carried out on each pump line (θ_P), the distribution network (θ_R) and deluge skid (θ_D). The cost of testing must only be considered once per group of components, since a pump line test examines the pump and all other elements on that line simultaneously, and a single ringmain and deluge skid test examines all associated components. It is assumed that the simultaneously tested components require the same specialized labor (C_{HT}) and the same test time (H_T) as all other elements. Therefore, the FDS testing cost (*STC*) can be evaluated as:

$$STC = TCFPL + TCAPL + TCR + TCDS, \qquad (5)$$

where *TCFPL*, *TCAPL*, *TCR* and *TCDS* denote the cost of testing the firewater pumps and lines, the cost of testing the AFFF pumps and lines, the cost of testing the ringmain and the deluge skid respectively.

The FDS total life cycle cost (*LCC*) is evaluated by summing all mentioned costs, i.e.

$$LCC = SIC + SCMC + SPMC + STC\ . \qquad (6)$$

5.2 ISPEASSOP Part 2

This part of the program is responsible for FDS unavailability and spurious fault trees construction for each design, their conversion to binary decision diagrams and calculation of the FDS unavailability and spurious trip frequency.

FDS unavailability: The fault tree combined with binary decision diagrams for quantification have been implemented. No explicit objection function exists, as altering the parameters in the design continually alters the structure of the fault tree and hence the logic function. Therefore, each possible design alternative is obtained from a single fault tree by using house events. Figure 3 shows the structure of the part of the fault tree that deals with two pump failure (gates G5-G7 need to be further developed).

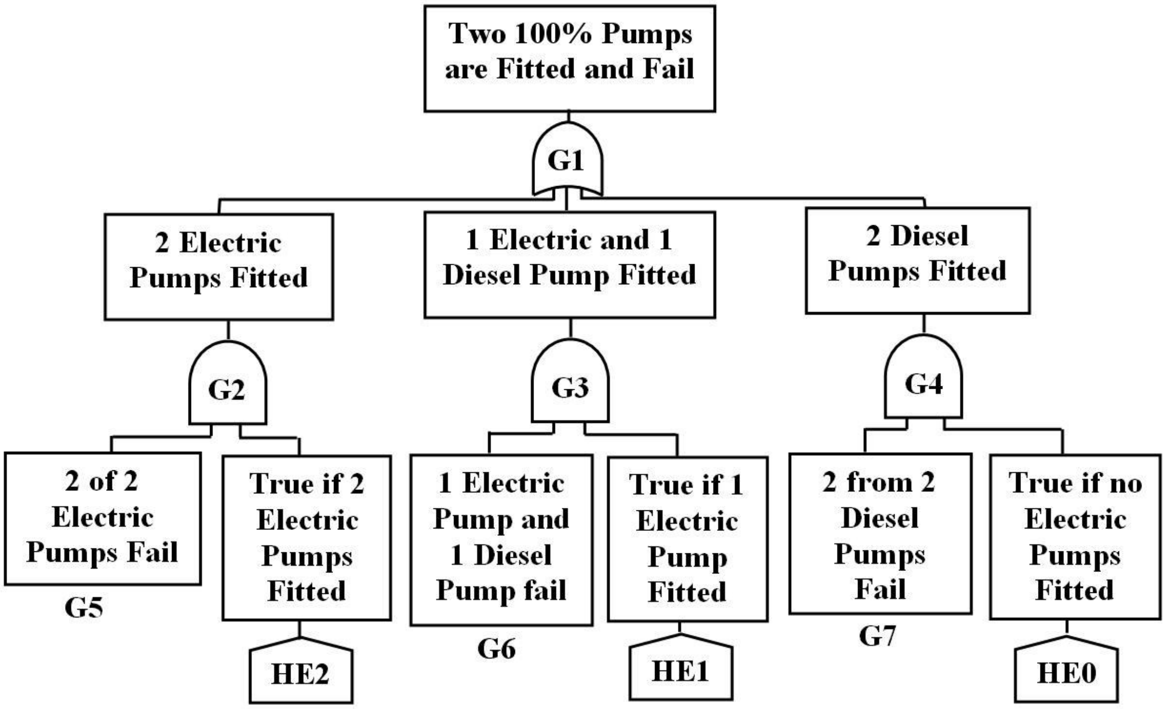

Two 100% Pumps are Fitted and Fail
G1
2 Electric Pumps Fitted
1 Electric and 1 Diesel Pump Fitted
2 Diesel Pumps Fitted
G2
G3
G4
2 of 2 Electric Pumps Fail
G5
True if 2 Electric Pumps Fitted
HE2
1 Electric Pump and 1 Diesel Pump fail
G6
True if 1 Electric Pump Fitted
HE1
2 from 2 Diesel Pumps Fail
G7
True if no Electric Pumps Fitted
HE0

Fig. 3 The fault tree structure for pump option.

If two electric pumps are fitted the house event, HE2, corresponding to this condition is set to TRUE. In this case house events HE1 and HE0, corresponding to the ‘one electric pump fitted’ and ‘no electric pumps fitted’, are conversely set to FALSE. Therefore, the right-most branches are switched off and a contribution to the top event arises from the left-most branch only. After the house event reduction, each fault tree is then converted to its BDD equivalent and integrated within the SPEA2 source code (section 5.3).

The top event ‘Firewater Deluge System Fails to Protect’ represents the causes of the firewater deluge system unavailability. There are three main reasons for the top event to occur, either the firewater or AFFF pump mechanisms are not activated, the AFFF pumps themselves fail or the water or foam deluge systems fail. The first reason, i.e. failure to initiate the firewater and AFFF pump mechanisms, occurs if both automatic and manual interventions fail. The manual start of the system fails if either the push button on the MFGP fails or if the operator fails to push the button. An automatic start fails if either the fire pump selector unit fails or the low pressure sensing on the firewater ringmain fails. Failure of the low pressure sensing depends on the number of pressure transmitters fitted (*N*) and the number of pressure transmitters required to trip the system (*K*).

Failure of the AFFF or water deluge skid occurs if either events ‘Failure of the water deluge skid’ or ‘Failure of the AFFF Deluge Skid’ occur. The possible reasons for the event ‘Failure of the water deluge skid’ to occur are: the water spray isolation valves fail, the strainer nozzle becomes blocked or the deluge valve fails to open. Further development of the event ‘The water deluge valve fails to open’ involves two scenarios connected by OR logic, i.e. events that restrict activation of the deluge valve and failure of the deluge valve itself. ‘Failure to activate the water deluge valve’ can be caused by the failure of the signal to the solenoids, by the solenoid valves remaining energized or by the failure of the valmatic release valve. In a similar manner the event ‘Failure of the AFFF deluge skid’ is developed. The fault tree consists of 618 gates, 50 basic events and 59 house events.

FDS spurious trip frequency; According to the FDS system limitations a number of spurious system occurrences is permitted, i.e. $F_{sys} < 0.75$ (Table 1). Hence, the spurious activation of the FDS must be established by developing the specific fault tree to quantify causes of this failure mode. The top event ‘Firewater deluge system fails spuriously’ occurs if the solenoid valves fail spuriously, the valmatic release valve opens spuriously or the signal from the main fire and gas panel to the solenoid valves is interrupted. The latter event occurs as a result of spurious activation of the ringmain pressure sensors.

Constant failure rates are assigned to all components from the FDS spurious trip fault tree. Furthermore, spurious failures are instantaneously revealed and repair initiated, hence the probability of failure of each basic event is independent of its associated maintenance test interval. Similarly to the unavailability fault tree, a single spurious trip fault tree with incorporated house events is formed to analyze each potential FDS design. After setting the house events, the resulting fault tree is converted to its BDD and the spurious s trip frequency is calculated within SPEA2 source code. The fault tree consists of 61 gates, 16 basic events and 13 house events.

5.3 ISPEASSOP Part 3

Step one of the algorithm is generation of the initial population, discussed in section 5.1. Step two requires fitness assignment. The FDS available resources are not inexhaustible (limitations are provided in table 1), therefore, penalty formulae must be derived to determine how large a penalty is required depending on the degree of violation of each constraint. The detailed penalty evaluations are given in [2]. Each penalty is subsequently added to the system unavailability to give the penalized system unavailability value (Q'_{sys}) for each possible FDS design.

Fitness assignment requires the division of the population of designs into dominated and nondominated groups according to the following rules: since the optimization is a minimization problem, the design *a* dominates the design *b* if all *a* parameter values are equal to or smaller than *b* parameter values and at least one of parameter *a* value is smaller that the respective *b* parameter value.

The design *a* is nondominated if there is no design in the population which dominates *a*. To avoid the situation that designs dominated by the same archive members have identical fitness values, for each individual both dominating and dominated solutions are taken into account. In detail, each design *i* in the archive and the population is assigned a strength value $S(i)$, representing the number of solutions it dominates. On the basis of the *S* values, the raw fitness $R(i)$ of a design *i* is calculated. This fitness is determined by the strengths of its dominators in both the archive and population.

Although the raw fitness assignment provides a sort of niching mechanism based on the concept of Pareto dominance, it may fail when most designs do not dominate each other. Hence, additional information is incorporated to discriminate between designs having identical raw fitness values. The density estimation technique used in SPEA2 is an adaptation of the *k*-th nearest neighbor method [5], where the density at any point is a decreasing function of the distance to the *k*-th nearest data point. In this problem the inverse of the distance to the *k*-th nearest neighbor is taken as a density estimate σ_{ij}, i.e. for each individual *i* the distances to all designs *j* in the archive and population. Obtained distances are stored in a list or matrix. After sorting the list in increasing order, the *k*-th element gives the distance sought, denoted as σ_i^k, where k is equal to the square root of the population size. Afterwards, the density $D(i)$ corresponding to i is defined by

$$D(i) = \frac{1}{\sigma_i^k + 2} . \tag{7}$$

In the denominator, two is added to ensure that its value is greater that zero. Finally, adding $D(i)$ to the raw fitness value $R(i)$ of the design *i* yields its fitness $F(i)$.

6 RESULTS

The objective of the design optimization problem for this system was to minimize three system optimization parameters (unavailability, spurious trip frequency and life cycle cost) by manipulating the design variables such that limitations placed on them by constraints are not violated. Ten ISPEASSOP runs, 100 generations each, have been implemented to tailor the algorithm parameters for the FDS system. Each run resulted in a Pareto set of 20 potential FDS designs. The number of non-dominated solutions in the Pareto front varied from 7 to 14 for different Pareto sets. Table 5 and 6 show the best FDS designs obtained after each run of ISPEASSOP. The best design was determined to be that with the largest number of smallest objectives.

Table 5 Best design variables after 10 runs of ISPEASSOP

Design Variables	Run Number 1	2	3	4	5	6	7	8	9	10
K/N	4/4	3/3	3/3	4/4	3/3	4/4	3/3	2/2	3/3	3/3
P	type2	type2	type1	type3	type3	type1	type1	type1	type3	type2
Firewater Supply and Distribution System										
F_E/F	3/5	2/4	1/1	2/3	1/1	1/1	1/1	3/4	2/6	3/6
F_P	33.3%	50%	100%	33.3%	100%	100%	100%	33.3%	33.3%	33.3%
F_T	type2	type1	type1	type2	type2	type1	type1	type1	type2	type2
AFFF Supply and Distribution System										
A_E/A	1/1	2/2	1/1	2/4	2/2	2/2	2/2	1/1	1/1	1/1
A_P	100%	50%	100%	50%	100%	100%	100%	100%	100%	100%
Valve and Material Types										
W	2	2	1	2	1	1	3	1	2	2
D	2	2	1	1	3	3	1	2	1	1
C	old	old	new	old	new	old	new	new	old	old
Maintenance Intervals										
θ_P	27	22	27	20	17	12	28	21	23	28
θ_R	5	1	21	21	19	18	24	18	22	20
θ_D	3	18	6	15	18	18	15	18	9	6
θ_{PM}	12	9	6	18	9	9	9	12	12	15

Table 6 Optimization parameter values for table 5

Run Number	LCC	$SCMC$	$SPMC$	STC	F_{sys}	Q_{sys}	Q'_{sys}
1	108641.00	20087.42	10290.97	8012.62	0.199976	0.008115	0.008115
2	119084.40	23113.32	12775.00	11346.08	0.200262	0.008181	0.008181
3	**73389.63**	18378.17	9672.50	4288.96	0.199977	0.008076	0.008076
4	122542.10	26101.96	7279.72	11110.40	0.200370	0.008181	0.008181
5	102773.80	36759.24	9571.11	7893.46	0.200540	0.008076	0.008076
6	105601.30	36759.24	9571.11	11120.91	0.200812	0.008076	0.008076
7	100919.40	36759.00	9571.11	4839.29	**0.199929**	0.008127	0.008127
8	101027.70	20315.44	8648.47	8513.77	0.200528	0.008149	0.008149
9	120858.20	21966.59	11832.08	9709.51	0.200228	0.008142	0.008142
10	122715.00	27214.55	9490.00	8060.42	0.199936	0.008029	**0.008029**

It can be noticed from table 6 that unavailability values for best designs of all ten runs are very close, however the smallest unavailability (Q'_{sys} = 8.029e-3) has been obtained in the last run. The third run of the program resulted in the system design with the smallest life cycle cost

(LCC = 73389.63 units). The smallest system spurious trip frequency has been obtained in 7th run (F_{sys} = 0.199929 times per year).

Table 5 shows that the majority of the designs have 3 pressure transmitters fitted and required to trip the system (N and K). The pressure transmitter type (P) varies. The firewater supply and distribution system usually consists of 1 or 4 pumps (F) of different type (F_T). 33.33% and 100% pump capacities (F_P) dominate. The AFFF supply and distribution system has 1-2 pumps (A) with 100% capacity (A_P). The difference between valve and material types (W, D and C) has insignificant effect on the design parameter values. For the majority of the designs the values of the maintenance test interval for the firewater and AFFF systems (θ_P) are in the range from 20 to 28 days. The maintenance test interval for the ringmain (θ_R) is usually higher than 20 weeks. On the other hand, values of the test interval for the deluge skid and preventative maintenance on components of wear-out type are in the interval [15, 18] and [9, 12] months respectively.

To establish the performance of the multi-objective approach these results are compared with those using a simple GA [2]. From the simple GA results the best design was determined as the one with the smallest unavailability. From the SPEA2 (ISPEASSOP program) the best design was determined to be that with the largest number of smallest objectives. Tables 7 and 8 provide the comparison of these best designs.

Tables 5-8 and show that all designs produced by ISPEASSOP have smaller unavailability and spurious trip frequency than the ones obtained by using the simple genetic algorithm. Designs 1-3 and 5-8 have also smaller life cycle cost. Using a simple GA sufficient genetic diversity among solutions in the population should be guaranteed. The relatively small initial population and small number of generations resulted in lack of such diversity and, therefore, better performance is produced by the SPEA2 method, due to its advanced feature (the archive) the algorithm doesn't loose valuable solutions during the search process. It might be expected that a significant increase in the number of generations or a larger initial population may make the simple GA produce better results than the SPEA2. However, another important advantage of the SPEA2 is that it finds optimal solutions faster, which is very important for large safety systems in terms of limited computer resources. One run of the simple GA takes several hours, on the other hand one run of the SPEA2 takes only 12 minutes. In addition, the SPEA2 allows minimization of more than one objective.

Table 7 Best FDS designs obtained by simple GA and SPEA2

Design Variables	GASSOP (GAs)	ISPEASSOP (SPEA2)
K / N	1 / 3	3 / 3
P	type 1	type 2
Firewater Supply and Distribution System		
F_E / F	3 / 6	3 / 6
F_P	50%	33.3%
F_T	type 2	type 2
AFFF Supply and Distribution System		
A_E / A	1 / 2	1 / 1
A_P	100%	100%
Valve and Material Types		
W	3	2
D	3	1
C	new	old
Maintenance Intervals		
θ_P	18	28
θ_R	1	20
θ_D	3	6
θ_{PM}	18	15

Table 8 Optimization parameter values for table 7

Optimization Parameters	GASSOP (GAs)	ISPEASSOP (SPEA2)
STC	8759.30	8060.42
SPMC	11123.80	9490.00
SCMC	29640.70	27214.55
LCC	120386.00	122715.00
F_{sys}	0.403000	0.199936
Q_{sys}	1.263e-2	8.029e-3
Q'_{sys}	1.263e-2	8.029e-3

100 generations of the algorithm explores approximately 3000 feasible possible system designs, which is a very small number compared to the total number of feasible designs (i.e., 56, 435, 097, 600). To test the performance of the developed technique further it was decided to increase the number of generations from 100 to 1500, which would explore more than 31000

potential system designs. The population of the 10th run has been chosen for this experiment since it produced the design with smaller system unavailability and spurious trip frequency compared to those obtained by the other runs. Figure 4 shows the comparison between Pareto fronts obtained after 100 and 1500 generations of the same initial population. The same fronts in two dimensional space are shown in Figure 5(a-c).

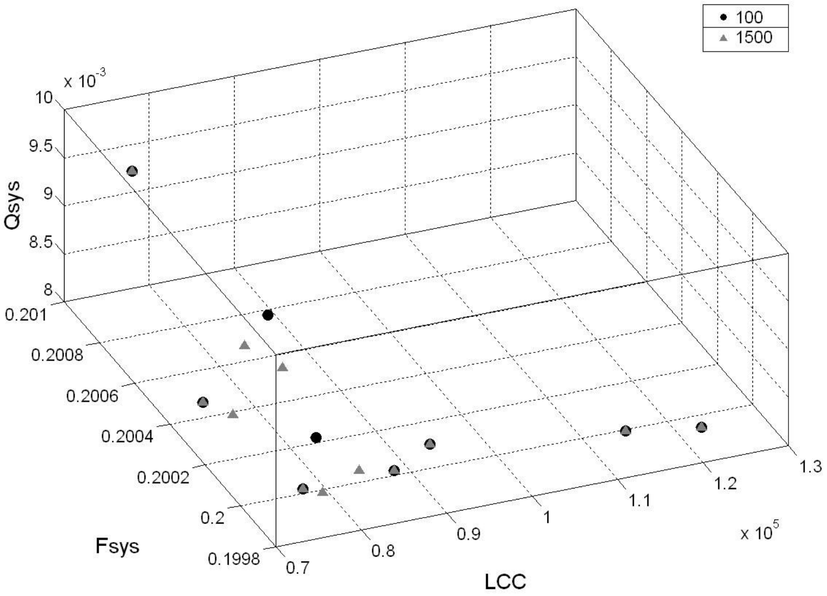
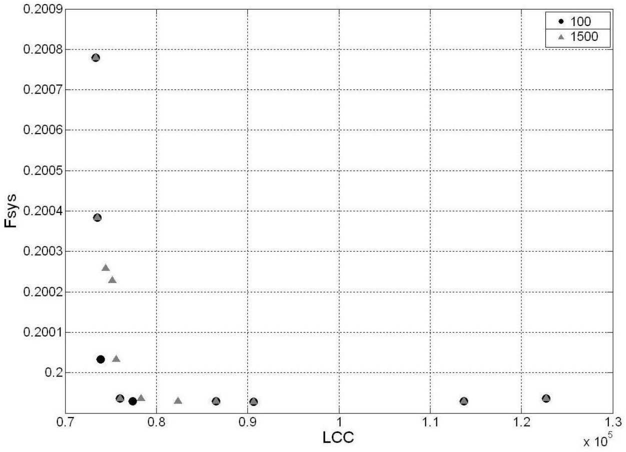
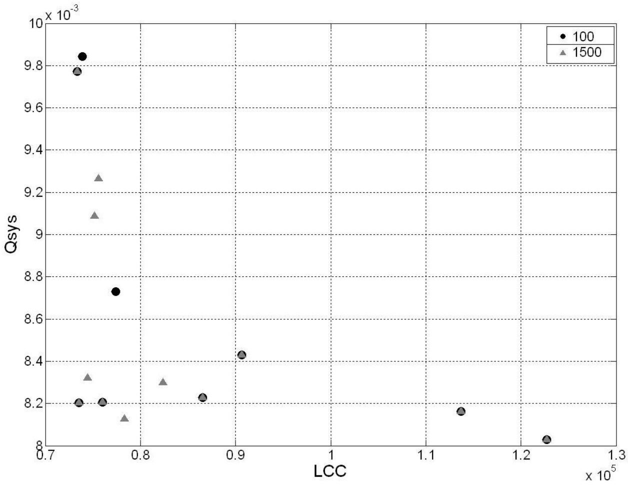


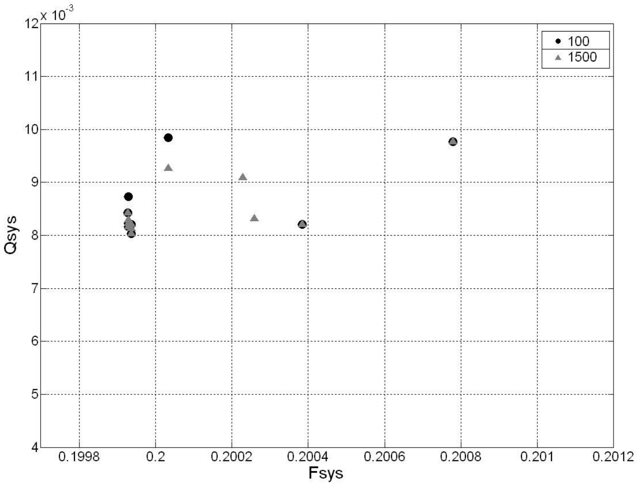
Fig. 4 Comparison of the Pareto fronts obtained after 100 and 1500 generations of the 10th run of the ISPEASSOP



a) Life cycle cost and spurious trip frequency



b) Life cycle cost and system unavailability



c) Spurious trip frequency and system unavailability

Fig. 5 Pareto front from figure 4 in a two dimensional space

Figure 4 shows that after 1500 generations several non-dominated solutions were added to the Pareto front, which are situated in the middle of the curve and, therefore, have provided balance between all optimization parameter values (i.e. all components are equally far from their global minimums). However, it can be seen from figure 5 that designs with minimal values of all optimization parameters have been found within the first 100 generations. Therefore, additional generations do not improve significantly the performance of the developed optimization technique. Additionally it can be noticed from figure 5 that an increase of system life cycle cost results in a decrease of system unavailability and spurious trip frequency (Fig. 5*a* and 5*b*). On the other hand, system unavailability and spurious trip frequency are directly proportional (Fig. 5*c*).

CONCLUSIONS

An automated robust design optimization process has been developed. The adequacy of the system performance in terms of unavailability calculation is assessed using fault tree analysis techniques. The causes of failure for each possible design alternative of a safety system is represented by a single fault tree by using house events. The use of the BDD technique allows the solution of the fault tree in the most efficient manner.

The developed tool has been successfully applied to the firewater deluge system, and produced good results for system design optimization. The SPEA2 produces improved results compared to those obtained by simple GAs. Another important advantage of the implemented technique is that it is faster and requires less memory resources. The performance of the developed technique in terms of limited computer resources has been tested by increasing the number of generations. However, this experiment improved the results only marginally.

It was assumed that the FDS consists of independent components. However, in reality one component failure may affect one or more other components. Therefore, the future work will be concentrated on testing the effectiveness of the technique on systems with dependencies.

REFERENCES

1. **Goldberg, D. E.** 1989. *Genetic algorithms in search. Optimization and machine learning*. Addison-Wesley publishing company, 1989.
2. **Andrews, J. D. & Bartlett, L. M.** 2003. Genetic algorithm optimization of a firewater deluge system. *Quality and reliability engineering international 19,* 2003, 39-52.

3. **Pukkala, T. & Kurtilla, M**. Examining the performance of six heuristic optimization techniques in different forest planning problems. *Silva Fennica Vol. 39, Issue 1*, 2005, 67-80.
4. **Chan, T. M. et al.** Resource management in wideband CDMA systems using genetic algorithms. *Applied Artificial Intelligence*, *Vol. 19*, 2005, 1-41.
5. **Zitzler, E. et a**l. *SPEA2: Improving the Strength Pareto Evolutionary Algorithm*. Computer engineering and communication network lab (TIK), report No. 103, 2001.
6. **Greiner, D. et al.** Safety systems optimum design by multiriteria evolutionary algorithms. *Springer-Verlag, EMO 2003, LNCS 2632*, 2003, 722-736.
7. **Hiroyasu, T.** *Diesel engine design using multi-objective genetic algorithm.* Report, Doshisha university, 2004.
8. **Martorell, S. et al.** A tolerance interval based approach to address uncertainty for RAMS+C optimization, *Reliability Engineering and System Safety*, *Vol. 92, Issue 4*, 2007, 408-422.
9. **Ben Aribia H. & Hadj Abdallah H.** Multi objective reactive dispatch optimization of an electrical network. *Leonardo Journal of Sciences, ISSN 1583-0233, Issue 10,* 2007, 101-114.
10. **Andrews, J. D. & Moss, T. R.** *Reliability and risk assessment. Second Edition.* Professional Engineering Publishing, 2002.
11. **Rauzy, A.** New algorithm for fault tree analysis. *Reliability engineering and system safety, Vol.40,* 1993, 203-211.
12. **Zitzler, E. & Thiele, L.** *An evolutionary algorithm for multi-objective optimization: The Strength Pareto Approach.* Computer engineering and communication network lab (TIK), report No. 43, 1998.

TABLES

ILLUSTRATIONS

APPENDIX

Notation

AFFF	aqueous film-forming foam
BDD	binary decision diagram
C_{HP}	Cost per hour of manual work to carry out preventative maintenance
C_{HR}	Cost per hour of manual work to repair failure (dormant or spurious)

C_R	Number of hours manual work required to repair the component
C_{SP}	Cost of spares each time preventative maintenance is undertaken
C_{SR}	Cost of spares for each repair carried out (dormant or spurious)
FDS	firewater deluge system
F_{sys}	spurious trip frequency
GAs	genetic algorithms
H_P	Number of hours manual work required to carry out preventative maintenance
LCC	life cycle cost
MOGA	a multi-objective genetic algorithm
Q_{sys}	system unavailability
Q'_{sys}	penalized system unavailability
SCMC	system corrective maintenance cost
SIC	system initial cost
SPEA2	improved strength Pareto evolutionary approach
SPMC	system preventative maintenance cost
STC	system testing cost