Genetic Algorithm Optimisation of a Firewater Deluge System

J.D.Andrews & L.M.Bartlett

Mathematical Sciences Department

Loughborough University

Loughborough

Leicestershire

LE11 3TU

Summary

Safety systems are designed to operate when certain conditions occur and act to prevent their development into a hazardous situation. Failure of a safety system for a potentially hazardous industrial system or process may have catastrophic consequences, possibly injuring members of the work force or public and occasionally resulting in loss of life. The purpose of this paper is to describe a design optimisation scheme using genetic algorithms applied to a firewater deluge system, which uses available resources to the best possible advantage to obtain an optimal safety system design.

Keywords: Optimisation, Genetic Algorithms, Safety Systems, Design

List of Symbols

HIPS High Integrity Protection System FDS Firewater Deluge System

AFFF	Aqueous Film-Forming Foam	MFGP	Main Fire and Gas Panel
λ_D	Dormant failure rate	λ_S	Spurious Failure Rate
τ_D	Dormant mean time to repair	τ_S	Dormant mean time to repair
N_S	Number of spares stored	C_I	Initial cost
C_S	Storage costs per component		
H_T	Number of man-hours work required to test component		
C_{HT}	Cost per hour of manual work to test component		
C_R	Number of man-hours work required to repair component		
C_{HR}	Cost per hour of manual work to repair failure (dormant or spurious)		
C_{SR}	Cost of spares for each repair carried out (dormant or spurious)		
H_P	Number of man-hours work required to carry out preventative maintenance		
C_{SP}	Cost of spares each time preventative maintenance is carried out		
C_{HP}	Cost per hour of manual work to carry out preventative maintenance		
β, η	Weibull parameters		

1. Introduction

The traditional engineering design process involves a trial and error type approach, where upon a design is created, analysed, and compared with a predetermined criterion of acceptability. If necessary the design is modified to meet the criteria, and the process is repeated. The end result is a design that is usually adequate rather than optimal. To find an optimal design a process is required which considers a number of design alternatives. One technique, which allows this type of parallel processing, is Genetic Algorithms [1].

However, difficulties occur in forming and solving the mathematical optimisation problem that represents a system design problem. One is that most, if not all, of the design variables are integer in form. Also, the constraints formed limiting the design to a practical solution are usually highly non-linear. This significantly restricts the class of mathematical techniques available to solve this problem. The potential of the genetic algorithm to optimise the design of a safety system has been demonstrated by application to a simple high integrity protection system (HIPS) [2]. The HIPS problem had only ten design variables. The application concerned with this paper is a firewater deluge system (FDS). The FDS is a larger, more complex system, which has in excess of 4.4×10^{10} design variations. Fault Tree Analysis [3] is used to determine the availability performance of the system, i.e. the probability it won't function on demand. This is the criterion on which the design will be assessed. The fault tree used to quantify this system failure probability has more than 450 gates and 420 basic events, and requires conversion to seventeen Binary Decision Diagrams [6], which facilitate a more efficient and accurate analysis procedure.

The remainder of this paper is divided into five sections, the first describing the firewater deluge system and the design considerations. The second looks at the means of analysis of the system, this is followed by the implementation of the genetic algorithm optimisation technique, and the final sections look at the results and conclusions.

2. Description of the Firewater Deluge System

To test the effectiveness of the optimisation process in dealing with larger design problems it has been applied to a Firewater Deluge System (FDS) on an offshore platform. The basic features of the deluge system are explained in the following subsections and a diagrammatic overview of the system is given in figure 1. Its function is to supply, on demand, water and foam at a controlled pressure to a specific area on the platform protected by a deluge system. As such, the FDS comprises a deluge skid, firewater pumps, associated equipment and ringmains, and Aqueous Film-Forming Foam (AFFF) pumps, with associated equipment and ringmains.

2.1 The Deluge System

The deluge valve set including 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 and its associated equipment act to spray water onto the affected area.

The deluge valve set comprises three main elements: the main distribution line, a water closing circuit and a control air circuit. Upon receipt of a signal from the Main Fire and Gas Panel (MFGP), the solenoid valves are de-energised and open, thus releasing air pressure from the control air circuit. The air pressure drop allows the valmatic release valve to open, and water from the water closing circuit runs to drain. This causes the

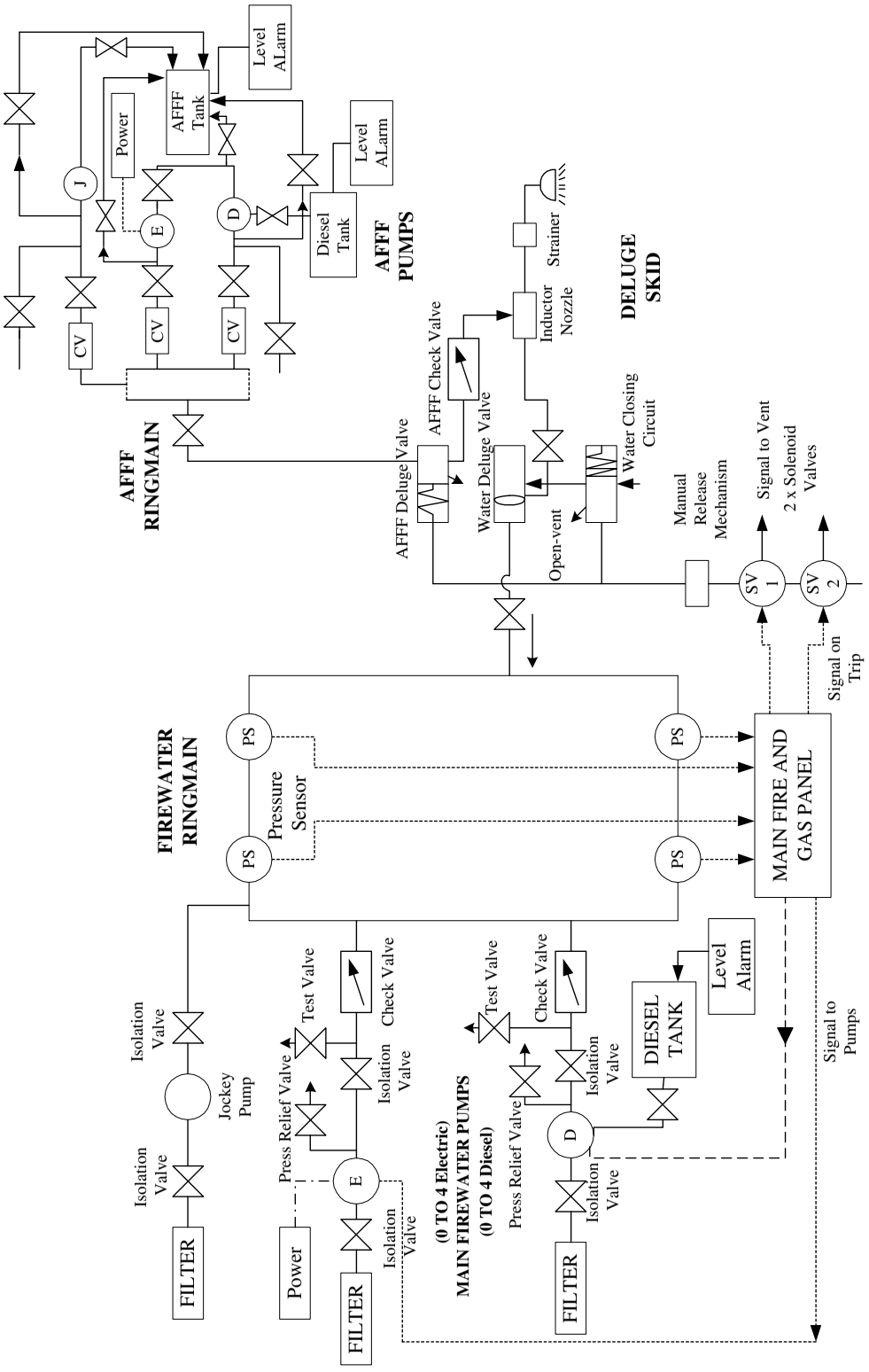

Figure 1: The Firewater Deluge System

pressure on the deluge valve diaphragm to fall. When the pressure on the diaphragm falls sufficiently, the firewater pressure acting on the underside of the deluge valve clack overcomes the load imposed by the diaphragm, allowing water to flow into the distribution pipes, through the nozzles and onto the hazard.

The system may also be operated manually by opening the system local manual release valve on the skid. This allows air to escape from the control air circuit and the system operates as described above.

The deluge valve set is also fitted with an AFFF supply line. Instrument air pressure maintains the valmatic release valve and AFFF valve closed. When the air pressure drops in the control air circuit, due to the solenoid valves being de-energised (the same components as those used to activate the water deluge valve), the AFFF valve and valmatic release valve open simultaneously. 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. The solution of water and approximately 3% foam then feed into the distribution network, through the nozzles and onto the hazard.

2.2 **Firewater Supply and Distribution System**

The deluge systems are connected to a pressurised ringmain network. The ringmain pressure is maintained by a jockey pump drawing water from the sea. Falling pressure is detected by the pressure transducers, which subsequently send a signal to the MFGP. In turn, the MFGP activates the firewater pumps to supply water direct from the sea at sufficient pressure to meet the deluge requirements. Pumps not needed remain in inactive standby. It is possible to start each pump manually, both locally and at the fire control panel.

The fire pumps are arranged in two sets, one set being powered from the main electric power plant and the other from their own dedicated diesel engines. The diesels have a tank size for a 24 hour supply. The tank has a low level alarm fitted, alarming in the Central Control Room.

2.3 AFFF Supply and Distribution

The foam concentrate is stored in a stainless steel tank and is distributed through a stainless steel ringmain network. The tank has a low level alarm fitted, alarming in the Central Control Room. The foam in the system is kept at approximately the same pressure as the firewater system by a continuously running air driven jockey pump. The AFFF pumps are either motor driven, supplied from the platform power plant, or diesel

driven. AFFF pumps start automatically when any firewater pump starts to supply foam at sufficient pressure to meet design requirements. Pumps not needed remain in standby. The diesel supply to the firewater diesel pumps is separate from that of the AFFF diesel pumps.

2.4 Design Variables

As regards the FDS it is necessary to determine the values for the design variables that represent the following:

- How many pressure transmitters on the ringmain (1,2,3,4)? N
- How many pressure transmitters are required to trip? K
- Which of three possible pressure transmitters types to select? P
- How many firewater pumps are required (1-8)? F
- Of these firewater pumps how many are electrically powered (0-4)? F_E
- What percentage capacity to choose for the firewater pumps (100%, 50% or 33 1/3%)? F_P
- Which of two possible pump types to select ? (For the 50% and 33 1/3% pumps only) F_T
- How many AFFF pumps are required (1-4)? A
- Of these AFFF pumps how many are electrically powered (0,1,2)? A_E
- What percentage capacity to choose for the AFFF pumps (100%, 50%? A_P
- Which of three possible water deluge valve types to select? W

- Which of three possible AFFF deluge valve types to select? D
- Which of two possible materials to use for certain components? C
- Maintenance test interval (MTI) for the firewater and AFFF pump system (1-28 days)? θ_P
- Maintenance test interval for the ringmain (1-24 weeks)? θ_R
- MTI for the deluge skid (3-18 months in 3 monthly intervals only)? θ_D
- Preventative maintenance on components of wear-out type (3-18 months in 3 monthly intervals only)? θ_{PM}

(Note each maintenance test interval, θ, is given in hours)

It should be noted that all pumps in the firewater system are to be of the same capacity, as are all pumps in the AFFF system. 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.

The design costs a certain amount to build, termed its initial cost. When in situ the FDS must be tested at regular intervals. Any failures found must be repaired. In addition, certain components are of wear-out type, and these must undergo preventative maintenance at regular intervals. For those components with non-constant failure rate the wear out phase of the bath-tub curve applies and thus the time to failure distribution used is the Weibull distribution. Knowledge of the components comprising the FDS enable predictions to be made about the expected cost of the system testing, repairs and

maintenance effort. The initial cost plus cost of maintaining the system yield the life cycle cost. Data is available for all components in the FDS, however the data for a subset of these is shown in tables 1 and 2. The event abbreviations refer to the following:

WV1	Water Deluge Valve Type 1 Fails to Open
WV2	Water Deluge Valve Type 2 Fails to Open
WV3	Water Deluge Valve Type 3 Fails to Open
AINBo	The foam supply into the firewater distribution line is blocked by inductor nozzle, old type material
AINBn	The foam supply into the firewater distribution line is blocked by inductor nozzle, new type material
AV1	AFFF Deluge Valve Type 1 fails to open on demand
E100	Failure of Electric Pump with 100% capacity
D100	Failure of Diesel Pump with 100% capacity
PT1	Failure of ringmain pressure sensor type 1 to indicate low ringmain pressure
PT2	Failure of ringmain pressure sensor type 2 to indicate low ringmain pressure
AE100	Failure of AFFF electric pump with 100% capacity
AD50	Failure of AFFF diesel pump with 50% capacity

Data contained in this table includes: The dormant failure rate (λ_D) and mean repair time (τ_D), spurious failure parameters (λ_S, τ_S) and the costs and effort associated with maintenance activities (see list of symbols).

Event	λ_D	τ_D	λ_S	τ_S	H_T	C_{HT}	C_R	C_{HR}	C_{SR}	N_S	C_S	C_I
WV1	4.0e-5	1.8e-5			2	30	18	30	200	2	200	400
WV2	3.5e-5	1.8e-5			2	30	18	30	250	2	200	500
WV3	2.8e-5	1.8e-5			2	30	18	30	300	2	200	600
AINBo	3.0e-5	1.2e-5			2	30	12	30	100	3	300	1000
AINBn	5e-6	1.2e-5			2	30	12	30	300	3	300	3000
AV1	4.0e-5	1.8e-5			2	30	18	30	150	2	150	300
AV2	3.5e-5	1.8e-5			2	30	18	30	200	2	150	400
AV3	2.8e-5	1.8e-5			2	30	18	30	250	2	150	500
PT1	7e-6	4e-6	7e-6	4e-6	1	45	4	45	50	2	100	500
PT2	1.4e-5	4e-6	1.4e-5	4e-6	1	45	4	45	20	2	100	200

Table 1: Data for subset of components in FDS.

Event	β	η	H_T	C_{HT}	C_R	C_{HR}	C_{SR}	H_P	C_{HP}	C_{SP}	N_S	C_S	C_I
E100	2	16667	2	30	72	30	1500	72	30	300	1	1000	3000
D100	2	14035	2	30	72	30	1450	72	30	290	1	1000	2900
AE100	2	16667	2	30	72	30	750	72	30	150	1	800	1500
AD50	3/2	20000	2	30	48	30	375	48	30	75	2	600	750

Table 2: Subset of Pump Data for FDS

Pumps are considered to deteriorate with time and times to failure are specified by the Weibull distribution with shape parameter β and characteristic life η. The values of these parameters are given, for a subset of the pumps, in table 2.

The choice of design is not unrestricted. Limitations have been placed on the design such that:

1) Total life cycle cost must be less than an average of 125000 units per year (i.e. initial cost plus total cost of maintenance, part 4 stated below).
2) Total cost of testing the system must be less than 20500 units per year.
3) Total cost of preventative maintenance effort must be less than 13500 units per year.
4) Total cost of maintenance effort must be less than 44000 units per year (i.e. cost of corrective maintenance due to repair of dormant and spurious failures plus 2 and 3 stated above).
5) The number of times that a spurious system shutdown occurs would be unacceptable if it were to occur on average more than 0.75 times per year.

3 Safety System Analysis

The FDS is a primary safety system on the platform designed to mitigate the consequences of pool fires, in addition to reducing overpressures in the event of an explosion. Failure in the event of a hydrocarbon release could result in fatalities. It is

imperative, therefore, that the FDS works when the demand arises. Thus, the objective is to minimise system unavailability whilst giving consideration to the available resources.

3.1 Evaluating the System Unavailability

There are a number of techniques commonly used for system unavailability assessment, for example, fault trees [3], reliability networks [4], Markov analysis [5], and simulation [5]. Due to its clear documentation procedures, which facilitates a more accurate failure logic development, the fault tree analysis approach has been adopted for use in this application. Analysis of the fault tree is carried out using the latest development of the Binary Decision Diagram [6-10]. No explicit objective function exists, as altering the parameters in the design continually alters the structure of the fault tree and hence the logic function. A single fault tree using house events is, therefore, constructed to model each possible design alternative (methodology discussed in section 3.1.1). This fault tree is then converted to its Binary Decision Diagram (BDD) equivalent and integrated within the Genetic Algorithm source code (discussed in section 5) to achieve optimal system performance.

3.1.1 House Events

House events can be used to enable 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.

Consider for example, the choice of a valve type, V1, V2 or V3. The structure of the part of the tree that deals with valve failure is shown in figure 2. If valve type 1 is selected the house event, H1, corresponding to the selection of this valve is set to TRUE. House events H2 and H3, corresponding to the selection of valves 2 and 3 are conversely set to FALSE. A contribution to the top event arises from the left most branch only. The two right most branches are in effect switched off. Levels of redundancy are handled in a similar manner.

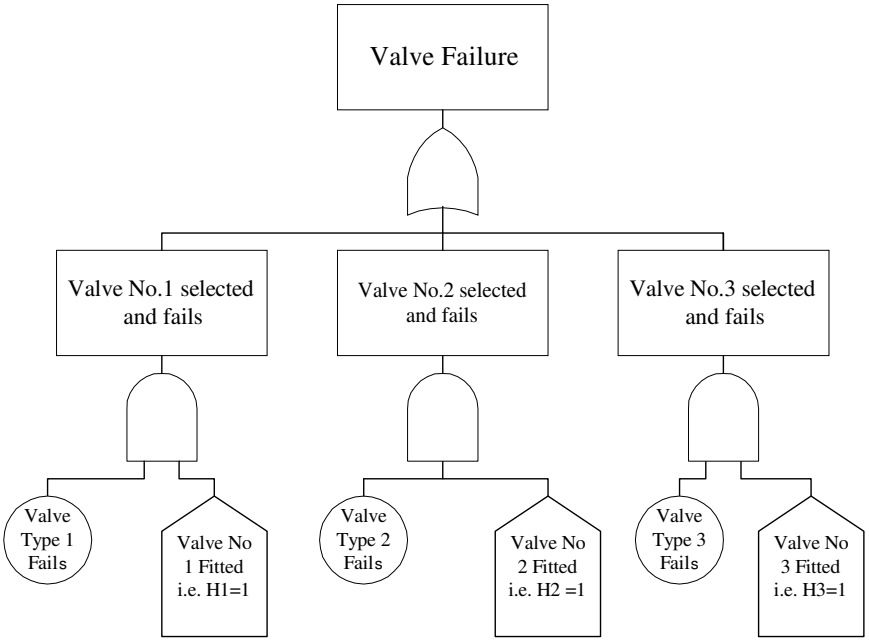

Figure 2: Fault Tree Structure for Valve Options

3.1.2 Construction of the System Unavailability Fault Tree

The top event of the fault tree representing the causes of system unavailability is defined as "Firewater Deluge System Fails to Protect". This top event will occur if either the firewater or AFFF pump mechanisms are not activated, the firewater or AFFF pumps themselves fail or the water or foam deluge systems fail, as indicated in figure 3. The FDS system unavailability fault tree construction is described via development of each of these sub-events in turn.

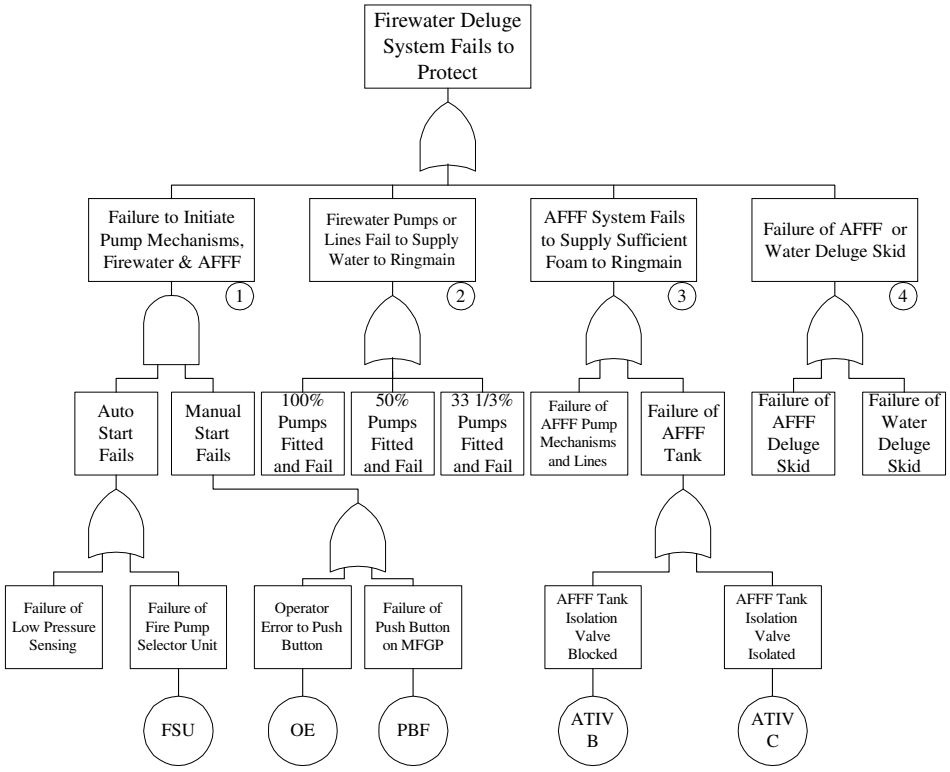

Figure 3: Firewater Deluge System Fails to Activate on Demand

Failure to Initiate Pump Mechanisms (Firewater and AFFF) – Event 1

Failure to initiate the firewater and AFFF pump mechanisms occurs if both automatic and manual starts fail. 'Manual Start' fails if either the push button on the MFGP fails or if the operator fails to push the button. 'Auto 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). House events are used to model each possible design alternative in the fault tree section below "Failure of Low Pressure Sensing".

Firewater Pumps and Lines Fail to Supply Water to Ringmain– Event 2

The FDS fails to supply sufficient water to the ringmain if failure of the firewater pump mechanisms or lines mean that the pumps of whatever capacity used cannot supply the required pressure. Events resulting in this scenario depend on the values assigned to the variables F_P, F, F_E, and F_T. 'Failure of Firewater Pumps or Lines' will occur if either the firewater pumps are of 100% capacity and fail, if firewater pumps are of 50% capacity and less than two are functioning, or if firewater pumps are of 33 1/3% capacity and less than three are functioning. These options are again developed in the fault tree by use of House Events.

AFFF System Fails to Supply Sufficient Foam to Ringmain – Event 3

The AFFF pump system fails to supply sufficient foam to the ringmain as a result of failure of the AFFF pump mechanisms or lines or isolation of the AFFF tank.

Failure of the AFFF or Water Deluge Skid – Event 4

'Failure of the AFFF or Water Deluge Skid' occurs if either 'Failure of the Water Deluge Skid' or 'Failure of the AFFF Deluge Skid' occur. Considering the former event, 'Failure of the Water Deluge Skid' occurs if either of the water spray isolation valves fail, the strainer or nozzle becomes blocked or the deluge valve fails to open. Developing further 'The Water Deluge Valve Fails to Open' requires consideration of the events that restrict activation of the deluge valve or failure of the deluge valve itself. 'Failure to Activate the Water Deluge Valve' occurs if the signal to the solenoids fails, both fitted solenoid valves remain energised or the valmatic release valve fails. 'Failure of the AFFF Deluge Skid' is developed in a similar manner. It differs primarily in that the blocked nozzle is replaced by blockage of the inductor nozzle and the strainer by a blocked AFFF check valve in the sequence of events described above.

4. Evaluation of System Performance Parameters

4.1 Frequency of Spurious Trip Occurrence of the FDS

As a result of the constraint limiting the number of spurious system occurrences permitted, the spurious activation frequency of the FDS must be established. No explicit expression can be defined which gives the trip frequency as a function of the design variables. This parameter requires an analysis to be performed on each specified design to be considered. As such a fault tree to quantify causes of this failure mode must first be developed.

The top event occurs if either of the solenoid valves fail spuriously, the valmatic release valve opens spuriously or the signal from the MFGP to the solenoid valves is interrupted. The latter event occurs as a result of spurious trip induction of the ringmain pressure sensors.

All components featured in the spurious trip fault tree for the FDS are ascribed constant failure rates. In addition, 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. Thus, a single fault tree is formed, which incorporates house events, to analyse any potential design. As with system unavailability quantification, the fault tree logic diagram is converted to a BDD form. Frequency calculations are performed as detailed in reference [10].

4.2 Life Cycle Costs

Constraints are imposed on the FDS, to limit the design to one which can be built and supported within the available financial resources. To build the FDS an initial cost is incurred. Once built further running costs must also be taken into account. In this study the running costs considered will be restricted to the maintenance activity, i.e. the cost of system testing at regular intervals, and the cost of preventative maintenance carried out on components that exhibit wear-out (servicing) i.e. increasing hazard rate. Each component has an initial purchase cost. A spares storage cost is also associated with each component, which depends on the number of spare items stored and the cost to store each item. The cost of corrective maintenance for each component depends on the expected number of failures and the cost to repair each failure. Specifically, corrective maintenance costs for component *i* (CM_i) is given by:

$$CM_i = (W_i^D + W_i^S) \times (H_T \times C_{HR} + C_{SR})$$

where W_i^D and W_i^S denote the expected number of dormant and spurious failures for component *i* respectively over the anticipated system life period. H_T, C_{HR} and C_{SR} refer to the number of man-hours work required to repair the component, the cost per hour of the work and the cost of spares for each repair carried out, respectively.

A component with a constant failure rate does not experience wear-out throughout its lifetime. At any time it is equally as likely to fail as when it was new and as such, preventative maintenance is not performed. The preventative maintenance cost incurred by a non wear-out component, is therefore, zero. Establishing the cost incurred by the FDS due to preventative maintenance (SPM) involves the summation of the preventative maintenance cost incurred by each fitted pump, since these were the only components considered to exhibit wear-out characteristics. The preventative maintenance (servicing) cost per year of each wear-out component depends on the number of times preventative maintenance is carried out in the year and the cost per time. Preventative maintenance cost incurred by component *i* (PMC_i) is, thus:

$$PMC_i = \left(\frac{8760}{\theta_{PM}}\right)(H_P \times C_{HP} + C_{SP})$$

where H_P, C_{HP} and C_{SP} correspond to the number of man-hours work required to carry out preventative maintenance, the cost per hour of the work and the cost of spares each time preventative maintenance is undertaken, respectively.

Tests can be carried out to examine different aspects of system performance, these range up to a full test which allows the water to flow into the tested area. Due to the inconvenience this will cause, tests short of full activation are more frequently performed. In this system tests are carried out on each pump line, the distribution network and deluge skid as dictated by θ_P, θ_R, and θ_D respectively. A pump line test examines the pump and

all other components on that line simultaneously. Similarly, a single ringmain and deluge skid test examines all associated components. The cost of testing must only be considered once per group of components. As such, the cost incurred due to system testing per year (STC) is given by:

$$STC = TCFPL + TCAPL + TCR + TCDS$$

where TCFPL, TCAPL, TCR, and TCDS represent 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 cost of testing the deluge skid respectively.

5. Genetic Algorithms for System Design Optimisation

John Holland developed Genetic Algorithms (GA's) in the 1970's at the University of Michigan. GA's are a class of optimisation procedures, which use principles mimicking those of natural selection and genetics, specifically genetic inheritance. Prior to the application of the GA the user must determine a representation scheme, define the fitness measure, define the parameters and variables for controlling the algorithm and designate a performance measure and a criterion for terminating a run.

The usual representation scheme for the GA is that each potential solution is coded as a string of parameter values, usually in binary code. The method then works with a population of strings. Following initialisation of the population of potential optimisation

problem solutions, usually randomly generated, the evaluation phase occurs. This phase requires a criteria to determine how 'good' a potential solution is. An objective function is generally used to provide a measure of how the potential design will perform, in this study this is achieved by quantifying the unavailability fault tree with house events set to represent that design. This value is then penalised to account for any constraint violations. The value of this penalised unavailability is referred to as the 'fitness' of the string. Following the evaluation of a population of strings, operators act to select, recombine and mutate the population, which evolves over subsequent generations.

The first operator is ***selection***. The purpose of selection is to increase the probability of reproducing strings that have higher fitness values, thus directing the search towards promising regions in the search space, the set of all possible design alternatives. Selection copies individuals without change into the next generation. The exchange of genetic material, sections of the string, occurs using the operations of ***crossover*** and ***mutation***. These operators allow new strings to be created and tested, for possible improvement in fitness.

Each safety system design is indicative of a specific set of parameter values (listed in section 2.4) representing a point in the search space. The genetic algorithm commences with a diverse population of designs. Each design's performance is evaluated using a preconceived criteria, in this case availability. The set of performance measures is subsequently used within a selection procedure to create a new population of candidate design solutions, which enable greater exploration of the search space. A second

iteration commences using this new population. Each iteration is termed a generation. The iterative procedure terminates after a pre-set number of generations.

6 Optimising the Firewater Deluge System

6.1 Methodology

Two binary strings were created to represent the variables which define a particular FDS design. The second string accommodates all maintenance test interval parameters, i.e. θ_P, θ_R, θ_D, θ_{PM}, and the first string all those parameters remaining. The first string is 29 bits in length, the second 16, as shown in figure 4.

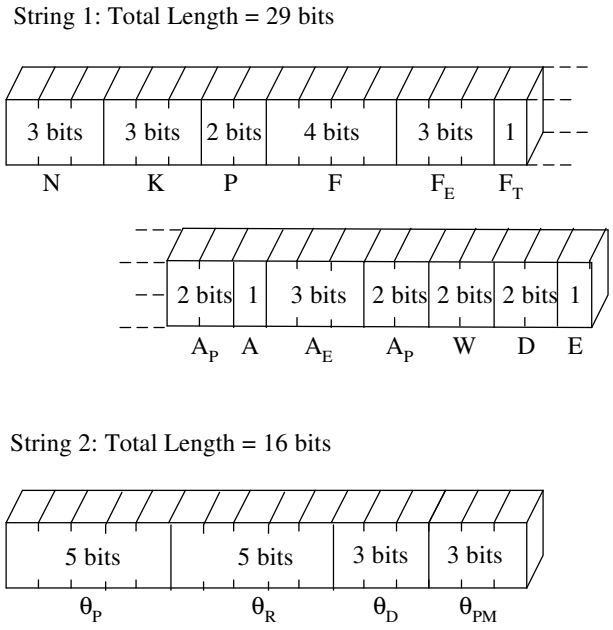

Figure 4: The FDS Parameter Set Coded as a Binary String

A simple explicit objective function to express the fitness or suitability of each deluge design does not exist. String fitness comprises of the system unavailability plus an imposed penalty should any of the constraints be violated. Penalty formulae must be derived to determine how big a penalty is required depending on the degree of violation of each constraint. The FDS has four constraints regarding cost. For each constraint a penalty formula is applied, equation (1) is used for excess life cycle costs (LCC_P), equation (2) for excess costs due to system testing (STC_P), and equations (3) and (4) for excess costs due to preventative maintenance ($SPMC_P$) and corrective maintenance ($TMEC_P$) respectively.

$$LCC_P = \left(\frac{\text{excess } LCC}{1250} \right)^{\frac{9}{8}} \times \left(\frac{Q_{SYS}}{100} \right) \quad (1)$$

$$STC_P = \left(\frac{\text{excess } STC}{205} \right)^{\frac{9}{8}} \times \left(\frac{Q_{SYS}}{100} \right) \quad (2)$$

$$SPMC_P = \left(\frac{\text{excess } SPMC}{135} \right)^{\frac{9}{8}} \times \left(\frac{Q_{SYS}}{100} \right) \quad (3)$$

$$TMEC_P = \left(\frac{\text{excess } TMEC}{440} \right)^{\frac{9}{8}} \times \left(\frac{Q_{SYS}}{100} \right) \quad (4)$$

The first term in each equation expresses the fraction by which the particular cost exceeds its permitted value. The system unavailability of the considered design is then multiplied

by the respective excess to establish the appropriate penalty. The term in these equations which expresses the excess resource over the permitted value is raised to the power of 9/8. This has the effect of providing a heavier penalty for larger violations. It was successful for this system.

Occurrence of a spurious trip ceases production on the processing platform and causes financial loss. As a result the spurious trip constraint violation is expressed in terms of cost. The life cycle cost constraint formula, equation (1), can then be used to derive the spurious trip penalty (S_P) applied to Q_{SYS}. Each penalty is subsequently added to the system unavailability to give a sole fitness for each design, i.e.

$$Q'_{SYS} = Q_{SYS} + LCC_P + STC_P + SPMC_P + TMEC_P + S_P$$

The constraint forms need to be simple and consistent in their derivation. The forms included here are specific to the FDS application. They would vary in form for other applications and, depending on the detail of information available, may be more detailed and precise in their formulation.

6.2 Results

To test the optimisation program which was produced in C, on a Unix station, 10 runs with a population of 20 strings over 100 generations were carried out. The mutation and crossover rate for each run was selected as 0.01 and 0.7 respectively. Each run required

several hours. The GA portrayed significant convergence in average population fitness, as can be seen in table 3, which shows the population average fitness value of the first and last generation of each run.

GA Run No	**Initial population average fitness**	**Final population average fitness**
1	0.177	0.0172
2	0.298	0.0306
3	0.332	0.0156
4	0.2	0.0297
5	0.164	0.0243
6	0.265	0.0223
7	0.186	0.0380
8	0.276	0.0218
9	0.238	0.0273
10	0.264	0.0232
Average Fitness		
Σ	0.24	0.025

Table 3: To Demonstrate Population Average Fitness Convergence

	Run Number									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
K/N	1/1	1/3	1/2	1/3	1/4	1/2	3/4	1/4	1/2	2/3
P	1	1	2	1	1	2	1	1	1	3
F_E/F	3/6	3/6	3/5	1/3	1/3	2/4	1/3	2/5	1/3	¾
F_P	50%	50%	100%	100%	100%	50%	100%	50%	100%	100%
F_T	1	2	1	2	1	2	2	1	1	2
A_E/A	1/2	1/2	1/2	2/4	2/4	2/4	2/4	1/2	2/4	1/2
AP	100%	100%	100%	50%	50%	50%	50%	100%	50%	100%
W	3	3	3	2	3	3	3	1	2	2
D	3	3	2	3	3	2	3	3	3	2
C	2	2	2	2	2	2	2	2	2	2
θ_P	24	18	8	11	11	23	13	16	27	8
θ_R	1	1	3	1	1	1	1	1	1	1
θ_D	3	3	3	3	3	3	3	3	3	3
θ_{PM}	18	18	15	15	18	18	15	12	18	18
Q'_{SYS*}	1.267	1.263	1.292	1.3	1.295	1.376	1.295	1.32	1.32	1.3

* Values shown are $x10^{-2}$

Table 4: Characteristics of the Best Design

Table 4 shows the characteristics of the best design resulting from each run. The best overall design for the FDS arose in the 2nd run and has a system unavailability of 1.263 $x10^{-2}$. This design is over 98.73% available. The best design arising in the first run has

very similar characteristics. It differs primarily in that 1 as opposed to 3 pressure sensors are included and the firewater pump is of type 2. The lifecycle costs, spurious trip frequency (TFreq), system unavailability, penalised system unavailability and difference between lifecycle costs and constraint are given in table 5.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
STC	9222.8	8759.3	12683.8	11688.7	9740.6	9132.2	11688.7	12074.3	9740.6	8795.5
SPMC	8994.6	11123.8	17467.9	16543.5	16543.5	10224.5	14399.5	10819.6	8284.9	16294.6
TMEC	26934.3	29640.7	38272.8	34647.1	33135.9	28164.4	32502.4	29345.5	24876.6	339161.1
LCC	116480	120386	120795	123643	122231	125237	121598	109691	113871	106928
TFreq	0.29	0.403	0.4641	0.243	0.243	0.464	0.2189	0.243	0.342	0.219
QSYS	1.267e-2	1.263e-2	1.292e-2	1.3e-2	1.295e-2	1.374e-2	1.295e-2	1.32e-2	1.32e-2	1.2e-2
Q'SYS	1.267e-2	1.263e-2	1.292e-2	1.3e-2	1.295e-2	1.376e-2	1.295e-2	1.32e-2	1.32e-2	1.3e-2
LCC-12500	8520	4614	4205	1357	2769	-237	3402	15309	11129	18072
% diff	6.8	3.7	3.3	1.1	2.2	-0.2	2.7	12.2	8.9	14.4

Table 5: Fitness Values Corresponding to each Design in table 3.

7 Discussion of Results

Many similar parameter combinations are repeated throughout the best designs portrayed in table 4. As regards the deluge system, both the water and AFFF deluge valves are predominately of type 3. The pipe work is consistently of the new non-corrosion resistant material, i.e. type 2.

A recurring combination for the firewater pump system is the inclusion of 3 firewater pumps, 1 electrically powered and 2 diesel driven. As regards the AFFF pump system, two combinations repeatedly arising are the inclusion of 2 100% pumps, 1 electric and 1 diesel, and 4 50% pumps, 2 electric and 2 diesel. Typically, the fittest designs portray balance in the number of electric to diesel pumps, particularly those of 50% capacity.

Failure of the distribution network is consistently very low (in the magnitude $3x10^{-6}$). The contribution of this network to the overall system unavailability of the design, is therefore, less significant. This is a likely reason for the marked variety in K and N. The pressure transmitters are predominately of type 1, thus, preventing the number of spurious trip occurrences from exceeding its limit of 0.75 per year.

A strong pattern arises in the values assigned to the maintenance test interval parameters. The maintenance test interval for the ringmain is set as 1 week for all but one of the best designs. The deluge skid is consistently tested at 3 monthly intervals. In contrast, the test interval between preventative maintenance tends to be at the higher end of its range, i.e. 15 to 18 months. Greater variations exist regarding θ_P.

The total life cycle cost of each of the best designs approaches the limit of 125000 units. As portrayed in table 5, the majority of the best designs make almost optimal use of the available resources.

To review, this study has used a large industrial safety system, with a large number of design variables and a set of constraints. With the use of a genetic algorithm, an optimal design has been found, making the best use of the available resources. In conclusion, it has been demonstrated by this study that the use of the genetic algorithm optimisation procedure combined with the fault tree analysis approach is both an effective and practical means to find an optimal system design. This provides an alternative to conventional approaches which deliver a merely adequate design.

Acknowledgement

The authors would like to thank Rachel Pattison, formerly of Loughborough University, for her contribution to this work.

References

1. D. Goldberg, "*Genetic algorithms in Search, Optimisation and Machine Learning*", Addison-Wesley Publishing Company, 1989.
2. R.L.Pattison, and J.D.Andrews, "Genetic Algorithms in Optimal Safety System Design", *ImechE Proceedings, Part E. Journal of Process Mechanical Engineering*, vol. E3, 1999, p187-197.
3. J.D.Andrews, and T.R.Moss, "*Reliability and Risk Assessment*", Longman Scientific and Technical, UK, 1993.

4. R.Billinton, and R.Allan, "*Reliability Evaluation of Engineering Systems*", 2nd Edition, Pitman, 1993.
5. E.J.Henley and H. Kumomoto. "*Reliability Engineering and Risk Assessment*", Englewood Cliffs, 1981.
6. A.Rauzy, "New Algorithms for Fault Tree Analysis", *Reliability Engineering and System Safety*, Vol. 40, 1993, pp203-211.
7. R.M.Sinnamon, and J.D.Andrews, "Fault Tree Analysis and Binary Decision Diagrams", *Proceedings of 1996 Reliability and Maintainability Symposium*, Las Vegas, Jan 1996, pp215-222.
8. R.M.Sinnamon, and J.D.Andrews, "New Approaches to Evaluating Fault Trees", *Proceedings of ESREL 95 Conference*, June 1995, pp241-254.
9. R.M.Sinnamon, and J.D.Andrews, "Improved Efficiency in Qualitative Fault Tree Analysis", *Quality and Reliability International,* vol. 13, 1997, p293-298.
10. R.M.Sinnamon, and J.D.Andrews, "Improved Accuracy in Quantitative Fault Tree Analysis", *Quality and Reliability International,* vol. 13, 1997, p285-292.