ELSEVIER

PII: S0141-1187(96)00022-3

Applied Ocean Research **18** (1996) 13–27

0141-1187/96/$15.00

Safety based design and maintenance optimisation of large marine engineering systems

J. Wang[a], J.B. Yang[b], P. Sen[c] & T. Ruxton[a]

[a]*The Centre of Maritime and Offshore Operations, School of Engineering and Technology Management, Liverpool John Moores University, Byrom Street, Liverpool, L3 3AF, UK*
[b]*Department of Manufacturing and Mechanical Engineering, University of Birmingham, Birmingham, B15 2TT, UK*
[c]*Department of Marine Technology, University of Newcastle upon Tyne, Newcastle, NE1 7RU, UK*

(Received 23 March 1996; accepted 5 May 1996)

This paper presents a techno-economic modelling methodology that may be applied to the design and maintenance optimisation of large engineering systems based on safety analysis. The proposed methodology brings together risk and cost objectives into the decision making process for the improvement of design aspects and maintenance policies. Information produced using an inductive bottom-up safety analysis approach described in this paper is utilised to construct a techno-economic model. Multiple Objective Decision Making (MODM) techniques are then employed to process the constructed model. The results produced can assist designers in developing efficient designs that take into account the probabilistic risks, their possible consequences, maintenance cost, repair cost and design review cost. A technical example of an hydraulic hoisting transmission system of an offshore pedestal crane is presented to demonstrate the interaction between economic modelling and safety analysis and to indicate the potential use of this techno-economic modelling methodology in the design and maintenance decision making process of large marine and offshore engineering products. Copyright © 1996 Elsevier Science Limited

1 INTRODUCTION

During the past decade, safety analysis of large marine and offshore engineering products such as marine cranes and offshore topsides has attracted a great deal of public attention. This is because a marine or offshore engineering product is usually a large, expensive and complex engineering structure and a serious failure could cause disastrous consequences. The objective of safety analysis of large marine and offshore products is to ensure that the probabilities of occurrence of serious system failures, which could cause death or injury, damage or loss of property, and degradation of the environment, are minimised by evaluating all aspects of design from a safety viewpoint.[11,15]

Safety analysis of most large marine and offshore engineering products is usually based on international standards and classification society requirements (or the equivalent) which incorporate the necessary rules and codes implemented over the years and updated, often under public pressure, following catastrophic accidents. It is still most commonly applied (if applied at all) at the final stages of design for verification purposes. It is worth noting that deficiencies in many large marine and offshore product designs are only corrected after accidents have happened. Actually, many decisions based on safety analysis at the initial stages of design may have great impact on product safety, and many accidents could have been prevented if designs had been initiated with the great emphasis on safety.

The report on the inquiry into the Piper Alpha accident has identified the need for the involvement of safety analysis from the early design stages to minimise the inherent hazards of large offshore products.[2] It is suggested that a 'safety case' approach be required to achieve this by studying all the aspects of the safety of the plant or process in question and how the risks involved are to be minimised.[5] The 'safety case' approach is currently in use in offshore engineering and it is suggested that it be used in the shipping industry.[5] A 'safety case' should include sufficient particulars to demonstrate that[2]

- hazards with the potential to cause a major accident have been identified, and
- risks have been evaluated and measures have been taken to reduce them to As Low As Reasonably Practicable (ALARP).

A 'safety case' is suggested to include the identification of a representative sample of accident scenarios and the assessment of the consequences of each scenario together with an assessment in general terms of the likelihood of its happening using Qualitative Risk Analysis (QRA) so that all reasonably practicable steps can be taken to control risks. Techno-economic analysis is also suggested to prepare a 'safety case' in order to incorporate safety aspects into the design process from the initial stages. The information produced using QRA methods such as Fault Tree Analysis (FTA) may be utilised to build a techno-economic model in order to optimise both design aspects and maintenance policies of a large engineering system within both economic and technical constraints so that safety can be considered as a criterion and safety analysis can move from an assessment function to a decision making function and finally to a verification function.[12]

Techno-economic modelling of large engineering systems has been extensively discussed,[1,3,6,7,10] but not many practical applications are reported. This could be largely because of the uncertain value placed on human life and the difficulties of qualifying risks.[5] However, it has been noted that if the uncertainty regarding the risks of a large marine or offshore product is not unacceptably high, a techno-economic analysis may be beneficially carried out to process the safety information produced and to make design decisions.

Safety and cost are obviously two conflicting objectives, with higher safety leading to higher cost. It is generally impossible to have a design which could maximise safety (i.e., minimise risks) and minimise the life cycle cost simultaneously. A compromise is therefore required. The decision as to which objective is to be stressed is dependent on the particular situation in hand. The appropriate level of safety then becomes dependent on the relative importance of the two criteria. If the non-dominated design options for such a situation have to be obtained, it becomes feasible to use a formal Multiple Objective Decision Making (MODM) tool to arrive at efficient or optimal decisions. This is what this paper aims to do.

In this paper, an inductive bottom-up safety analysis approach is presented in which Failure Mode, Effects and Criticality Analysis (FMECA), Boolean Representation Modelling (BRM) and Monte Carlo simulation method are used in an integrated way. Such an inductive approach may be very suitable to the safety analysis of large marine and offshore engineering products because of their characteristics such as the non-existence of historical failure data, the impracticability of full-scale experimentations, complex interactions between their subsystems, and the difficulty of replacements or modifications once on location and in operation.[12] This inductive approach may give a higher level of confidence that all system hazardous states (top events) and the respective causes are identified, especially for those marine and offshore products with a comparatively high level of innovation. A techno-economic modelling methodology is then proposed to interrelate economic modelling and safety analysis to formulate a techno-economic model in which both risk and cost objectives are involved. The formulated model takes into account both design aspects and maintenance activities. MODM techniques are then employed to process the constructed model to generate the best compromise maintenance policies and design review actions. A technical engineering example is finally presented to demonstrate the proposed techno-economic modelling methodology.

2 SAFETY ANALYSIS

2.1 Top-down and bottom-up safety analysis approaches

Safety analysis, as used for the assessment of risks associated with an engineering system or product, may be summarised to answer the following four questions:

1. What can go wrong?
2. What are the effects and consequences?
3. How often will they happen?
4. What measures need to be undertaken to reduce the risks and how can this be achieved?

To answer the above questions it is required to examine an actual or proposed design to identify and assess potentially hazardous situations and associated risks in order to provide a rational basis for determining where risk reduction measures are required.

Either a top-down or a bottom-up safety analysis approach can be used to identify accident scenarios. The decision as to which kind of analysis is more appropriate is dependent on the availability of failure data of the product being studied, the indenture level of the analysis required, the degree of complexity of the inter-relationships of the components, subsystems, and the level of innovation.

A top-down safety analysis of a system starts with the identification of the top events which can be obtained from previous accidents and incident reports of similar products. After the top events required to be studied further have been determined, the causes associated with them are then identified deductively in increasing detail until all the causes are identified at the required level of resolution. An FTA is a typical top-down method which can effectively be integrated into the top-down safety analysis process.

For large marine and offshore products with a comparatively low level of innovation, a top-down safety analysis may prove convenient and efficient because it only deals with the failure paths leading to the system top events obtained from previous accidents and incident reports of similar products. Obviously, experience and good understanding of a marine or offshore product are very important for the efficient use of such an approach. However, for large marine and offshore products with a comparatively higher level of innovation, there may be a

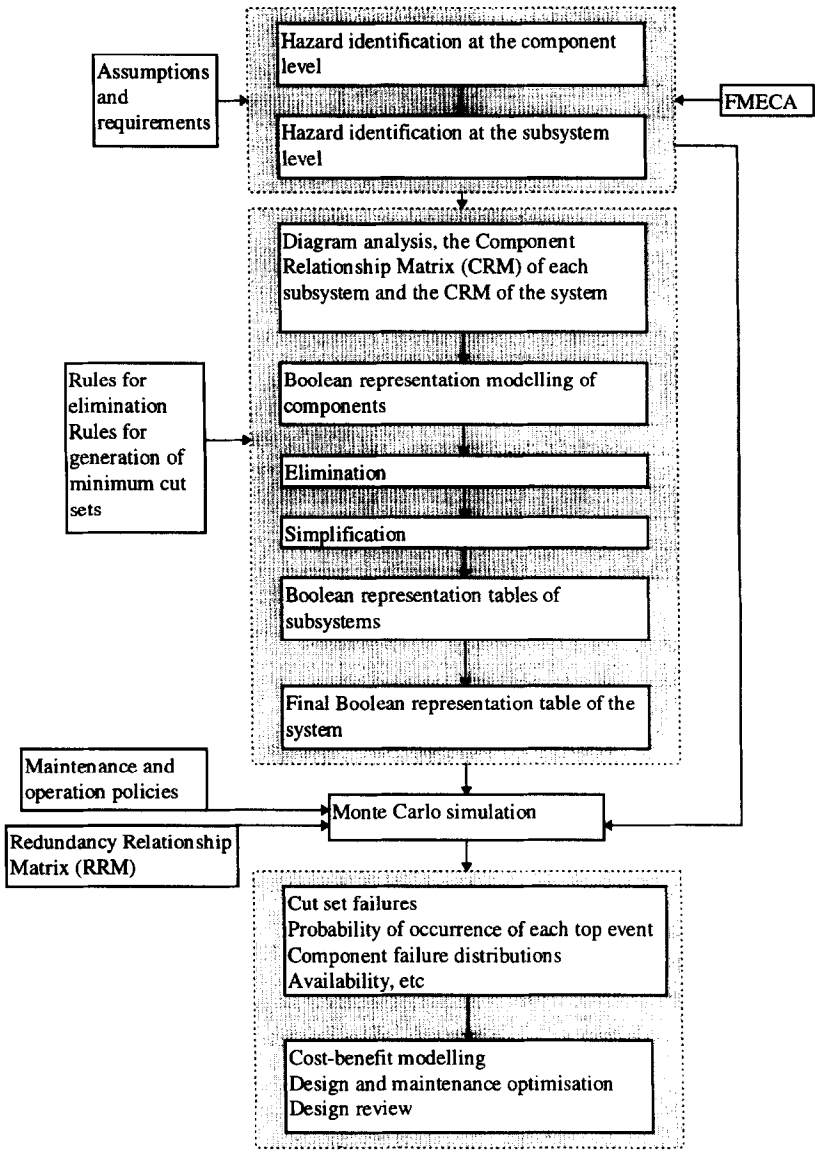

Fig. 1. An inductive bottom-up safety analysis process.

lack of knowledge or experience regarding the design solution and its possible effects on product safety. For such products, a top-down safety analysis may have the following problems:

1. Failure data (i.e., system top events) may not be available from previous accidents and incident reports of similar products.
2. Lack of confidence that all failure causes associated with the system top events are completely identified.
3. Deductive characteristics in a top-down safety analysis may not address the complex interactions present in a complex product address in an analytical way.

An inductive bottom-up safety analysis may therefore be expected. Such an analysis may be started from the component level, progressed up to the subsystem level, and finally to the system level. All of the top events and associated causes can be identified with a significant reduction of omissions using an inductive bottom-up safety analysis approach. Such an inductive approach incorporating Failure Mode, Effects and Criticality Analysis (FMECA), Boolean Representation Modelling (BRM) and Monte Carlo simulation is shown in Fig. 1. [15,18]

A large marine or offshore engineering system can be broken into subsystems which can be further broken down to the component level. After proper constraints and assumptions have been made, an FMECA can be carried out to identify the following information at the component level:[8]

- All potential failure modes and associated causes.
- The failure rate of each failure mode.
- Effects (consequences) on the safety and operability of the higher indenture levels (including the level analyzed).
- The severity class of the resulting effects where

each class may be defined as the following four standard degrees:[8]

1. Catastrophic: Involving death and or system loss.
2. Critical: Involving severe injury and/or major system damage.
3. Marginal: Involving minor injury and/or minor system damage.
4. Negligible: Involving no injury and negligible damage to the system.

The information produced from the FMECA at the component level can be used to assist in the construction of the Boolean representation table of each component.[18] The Boolean representation table of a component describes the conditions which must be satisfied for the occurrence of the identified component's output states.[15,17,18] The last column of the Boolean representation table describes the states of the output of the component while other columns prescribe the states of the input attributes. Each row is a prime implicant which represents a possible condition for an occurrence of the component's output state where a prime implicant can be considered to be the equivalent of a cut set in FTA but for systems with multiple state variables.[18] After a Component Relationship Matrix (CRM) has been constructed for a subsystem, the rules of elimination can be applied to substitute intermediate variables by primary variables and the rules of simplification to absorb and merge redundant rows and redundant attributes to simplify the table to an irreducible form.[4,18] After the Boolean representation tables of the subsystems have been constructed, an irreducible Boolean representation table of the system, in which all the input attributes are basic events, can be produced by applying the rules of elimination and simplification and studying the CRM of the system.[18] The obtained irreducible system Boolean representation table is not guaranteed to contain all the causes associated with the system output states since variables with multiple failure states are involved. The extra prime implicants can be produced out of the existing ones in the obtained irreducible table using Quine's algorithm theory.[4,18] After the produced extra prime implicants have been added to the obtained irreducible table and the rules of simplification have been applied again, the final system Boolean representation table is obtained which contains all the system top events and the associated minimum prime implicants (cut sets).[17,18] The probabilities of occurrence of the identified top events and the associated cut sets can be quantitatively estimated, on the basis of the obtained final system Boolean representation table, using the Monte Carlo simulation method with regard to Mean Time Between Maintenance (MTBM).[16] Revealed failures and covert failures can be taken into consideration.[16] The typical outputs from the simulation analysis of the obtained final system Boolean representation table are:[16]

- probability distribution of occurrence of each system top event with MTBM, and
- probability distribution of occurrence of each cut set with MTBM.

The component/subsystem failures can also be assessed by constructing a component/subsystem failure simulation model with regard to the component Redundancy Relationship Matrix (RRM).[16,17] Such a model can make use of the information produced from the FMECA. The typical outputs from such a simulation model are:[16]

- failure distributions of components with MTBM, and
- the availability of the system.

After the top events of the system have been identified, consequence analysis can be carried out to study the possible effects caused by the occurrence of each identified system top event. The possible consequences of a system top event can be quantified in terms of the possible loss of lives and property, and the degradation of the environment. They may best be quantified by experts regarding the particular operating situation in hand.

The information produced using the above described safety analysis approach can be used to build a techno-economic model in order to improve the safety of the system and to reduce the life circle cost of the system. In the remainder of this paper, a techno-economic modelling methodology will be presented in which both the probabilities of occurrence of the system top events and the costs of system failures, maintenance, repairs and design review actions over the product life time can be taken into consideration simultaneously.

2.2 Safety modelling

The occurrence of a system top event could cause serious consequences. The safety of a large marine or offshore engineering system can be improved by reducing the probabilities of occurrence of the system top events.

The occurrence of a system top event is completely dependent on the occurrence of the associated minimal cut sets. If one cut set failure occurs, the system top event happens. Therefore, a reduction of the probability of occurrence of a system top event is a matter of reducing or eliminating the probabilities of occurrence of the associated cut sets. The usual way of reducing the probabilities of occurrence of the system top events is to reduce or eliminate the probabilities of occurrence of some significant cut sets with relatively higher probabilities of occurrence since it is impractical and impossible to reduce or eliminate all the associated cut sets.

The probabilities of occurrence of the system top events and the associated minimal cut sets can be obtained using the described inductive bottom-up system safety analysis approach. It should be noted that such probabilities are functions of MTBM. The probabilities increase as the MTBM increases. Such probability functions are normally discrete and non-linear because failure probabilities may only be obtained by simulation at discrete MTBM values.

Suppose there are n system top events and P_i(MTBM) represents the probability of occurrence of the top event T_i. Suppose c cut sets are taken into account for reduction or elimination regarding all the system top events. Let P_{Dj}(MTBM) represent the original probability of occurrence of the jth cut set before a design review action is taken and ΔP_{Dj} represent the probability reduction of occurrence of this cut set as a result of a design review action. P_i(MTBM) and P_{Dj}(MTBM) can be obtained using the inductive bottom-up safety analysis approach as discussed in the last section.

The safety of the system can be improved by minimising the risks. If the reduction or elimination of one cut set does not significantly affect others, the risk function can be expressed as the sum of the probabilities of occurrence of the system top events and the c cut sets considered for reduction or elimination while each system top event is weighted on the basis of the severity of its possible consequences. Suppose *Risk* represents such a function. The safety model can be constructed as follows:

$$\min: \; Risk = \sum_{i=1}^{n} K_i \times P_i(\text{MTBM}) + \sum_{j=1}^{c} K_{Dj}(P_{Dj}(\text{MTBM}) - \Delta P_{Dj}$$

$$\text{subject to}: \; \text{MTBM}_{\max} \geq \text{MTBM} \geq \text{MTBM}_{\min}$$

$$0 \leq \Delta P_{Dj} \leq P_{Dj}(\text{MTBM}) \;\; (j = 1, 2, \cdots, c)$$

where K_i = the weighting factor representing the severity of top event T_i, MTBM_{max} = the largest MTBM value used in the safety analysis, MTBM_{min} = the smallest MTBM value used in the safety analysis and $K_{Dj} = K_i$ if the jth cut set is associated with top event T_i.

The first term of the risk function deals with the maintenance policies. This term represents the sum of the risks associated with the top events before the design actions are taken. The second term takes into account both the maintenance policies and the design review actions. This term represents the remainders of the risks associated with the c cut sets after the design review actions have been taken. The occurrence of the cut sets considered for reduction or elimination contributes to the occurrence of the system top events. Obviously, the smaller the sum of the two terms is, the higher the safety level of the system. It can be noted that some cut sets may be double accounted in the risk function. The purpose of modelling safety in such a way is to make sure that *Risk* is a monotonically increasing function of MTBM. Risk assessment is not affected by double accounting of some cut sets. The above safety model implies that the maintenance policies and the design review actions should be implemented to minimise the risks of the system.

3 ECONOMIC MODELLING

Cost is always an important issue in the design process of large marine and offshore engineering systems. The safety-related life cycle cost of a large marine or offshore engineering system may be modelled by taking into account the top event-caused consequences, repair cost, maintenance cost and design review cost. The following simplifying assumptions are made to implement economic modelling:

1. The basic diagram of the system to be analyzed is not changed.
2. Manpower and spare parts are sufficient for the repairs and maintenance activities.
3. All the subsystems return to their original conditions after a full maintenance.
4. Failed subsystems are repaired 'same as new' and the rest of the subsystems are not affected by the repairs.
5. Cost incurred is expressed as the present value.

The safety-related life cycle cost model is proposed as follows:

3.1 Top event-caused cost

A system may have several serious top events, each of which could result in a system breakdown and possibly cause serious consequences such as injury or loss of lives, damage or loss of property and the degradation of the environment. Top event-caused cost includes the following three parts:

C_{TC}: cost directly caused by the occurrence of the system top events.
C_{TL}: lost income due to the loss of the production ability.
C_{TR}: repair cost caused by the occurrence of the system top events.

Top event-caused cost $COST_T$ is given by:

$$COST_T = C_{TC} + C_{TL} + C_{TR}$$

$$C_{TC} = \sum_{i=1}^{n} C_{Ti} \times P_i(\text{MTBM})$$

$$C_{MP} = \sum_{i=1}^{n} C_{Li} \times P_i(\text{MTBM})$$

$$C_{MM} = \sum_{i=1}^{n} R_{Ti} \times P_i(\text{MTBM})$$

where:

C_{Ti} = cost directly caused by the occurrence of top event T_i.
C_{Li} = lost income caused by the occurrence of top event T_i.
C_{Ri} = repair cost caused by the occurrence of top event T_i.

3.2 Maintenance cost

Maintenance cost includes the following three parts:

C_{ML}: cost of labour.
C_{MP}: cost of parts.
C_{MM}: lost income during the periods of maintenance activities.

Maintenance cost $COST_M$ is given by:

$$COST_M = C_{ML} + C_{MP} + C_{MM}$$

$$C_{TC} = \sum_{k=1}^{\frac{T_{PT}}{\text{MTBM}}} C_{MLk} \quad C_{MP} = \sum_{k=1}^{\frac{T_{PT}}{\text{MTBM}}} C_{MPk} \quad C_{MM} = \sum_{k=1}^{\frac{T_{PT}}{\text{MTBM}}} C_{MMk}$$

where

C_{MLk} = cost of the labour required for the kth maintenance.
C_{MPk} = cost of the parts required for the kth maintenance.
C_{MMk} = lost income during the period of the kth maintenance.
T_{PT} = the project life time.
T_{PT}/MTBM = the number of major maintenance activities to be conducted over T_{PT}.

If $C_{MLi} = C_{MLk}$, $C_{MPi} = C_{MPk}$ and $C_{MMi} = C_{MMk}$ for $i = 1, 2$, T_{PT}/MTBM, and $k = 1, 2, \ldots, T_{PT}$/MTBM, $COST_M$ can be expressed as follows:

$$C_M = (C_{ML1} + C_{MP1} + C_{MM1}) \times \frac{T_{PT}}{\text{MTBM}}.$$

3.3 Repair cost

If a key component/subsystem in a system fails, the system should be shut down and the failed component/subsystem should be replaced or repaired immediately. Repair cost includes the following three parts:

C_{RL}: cost of labour.
C_{RP}: cost of parts.
C_{RR}: lost income caused by the loss of the production ability due to failures of the components/subsystems.

Repair cost $COST_R$ is given by:

$$COST_R = C_{RL} + C_{RP} + C_{RR}$$

$$C_{RL} = \sum_{i=1}^{m} C_{RLi} \times f_i(\text{MTBM})$$

$$C_{RP} = \sum_{i=1}^{m} C_{RPi} \times f_i(\text{MTBM})$$

$$C_{RR} = \sum_{i=1}^{m} C_{RRi} \times f_i(\text{MTBM})$$

where:

C_{RLi} = cost of the labour for repairing the ith subsystem.
C_{RPi} = cost of the parts for repairing the ith subsystem.
C_{RRi} = lost income caused by the loss of the production ability due to failures of the ith subsystem.
f_i(MTBM) = the number of failures of the ith component/subsystem, which is a function of MTBM and can be obtained using the approach described earlier.
m = the number of the components/subsystems.

3.4 Design review cost

Since the basic design diagram of the system is not changed, a design review may only involve the use of more reliable components or provision of protection systems, sensors and redundancies, or a combination of them, to reduce or eliminate the most significant cut sets associated with the identified system top events. Obviously, the more investment is directed at the system for the safety improvement, the higher safety level of the system can be achieved. A higher safety level of the system results in the lower probabilities of occurrence of the system top events, which lead to a less expenditure in the operation and maintenance process.

In the design review cost modelling, the following assumptions are made for the convenience of analysis.

1. The investment to be assigned to the system safety improvement first goes to the reduction or elimination of the cut sets (associated with the identified system top events) with relatively higher probabilities of occurrence.
2. After a design action has been taken to a cut set, other cut sets are not significantly affected.
3. The probability reduction of occurrence of a cut set is proportional to the amount of money assigned to this cut set.

Suppose M_j ($j = 1, 2, \ldots, c$) represents the cost required to eliminate the jth cut set in the design review process. The relationship between the amount of money assigned to this cut set (ΔM_j) and its probability reduction in occurrence (ΔP_{Dj}) can be described as follows:

$$\text{i.e. } \Delta M_j = \frac{\Delta P_{Dj}}{P_{Dj}(\text{MTBM})} M_j.$$

The cost incurred in the reduction or elimination of c cut sets in the design review process is given by:

$$COST_R = \sum_{j=1}^{c} \Delta M_j.$$

The elimination or reduction of the jth cut set can result in a probability reduction of occurrence of top event T_i if top event T_i is associated with the jth cut set. The possible benefit from the elimination or reduction of c cut sets is

given by:

$$Benefit = \sum_{j=1}^{c} \Delta P_{Dj} \times C_{Dj}$$

where $C_j = C_{Ti}+C_{Li}+C_{Ri}$ if top event T_i is associated with the jth cut set.

The total design review cost $COST_D$ is given by: $COST_D = COST_R$-$Benefit$

$$= \sum_{j=1}^{c} \Delta M_j - \sum_{j=1}^{c} \Delta P_{Dj} \times C_{Dj} = \sum_{j=1}^{c} \left(\frac{M_j}{P_{Dj}(\text{MTBM})} - C_{Dj}\right)\Delta P_{Dj}.$$

3.5 Operational cost

Average daily operational cost $COST_O$ is given by:

$$COST_0 = \frac{C_0}{365}$$

where C_O is the annual operational cost of the system.

The models concerned with top event-caused consequences, maintenance cost, repair cost and design review cost should be modified by taking into account the operational cost. The modified models are shown as follows:

$$COST_T^* = COST_T - COST_{OT} \quad COST_M^* = COST_M - COST_{OM}$$

$$COST_R^* = COST_R - COST_{OR} \quad COST_D^* = COST_D - COST_{OD}$$

$$COST_{OT} = \sum_{i=1}^{n} COST_O \times P_i(\text{MTBM}) \times BT_{Ti}$$

$$= COST_O \sum_{i=1}^{n} P_i(\text{MTBM}) \times BT_{Ti}$$

$$COST_{OM} = COST_O \times BT_{Mi} \times \frac{T_{PT}}{\text{MTBM}}$$

$$COST_{OR} = \sum_{i=1}^{m} COST_O \times f_i(\text{MTBM}) \times BT_{Ri}$$

$$= COST_0 \sum_{i=1}^{m} f_i(\text{MTBM}) \times BT_{Ri}$$

$$COST_{OD} = COST_0 \sum_{j=1}^{c} \Delta P_{Dj}(\text{MTBM}) \times BT_{Dj}$$

where:

$COST_T^*$ = top event-caused cost after the modification.
$COST_M^*$ = maintenance cost after the modification.
$COST_R^*$ = repair cost after the modification.
$COST_D^*$ = design review cost after the modification.
BT_{Ti}^* = the system breakdown time caused by the occurrence of the ith top event.
BT_{Mi} = the expected time required for the ith maintenance.
BT_{Ri} = the time required for repairing the ith subsystem.
BT_{Dj} = if top event T_i is associated with the jth cut set.

3.6 Economic modelling

An economic model is proposed to combine top event-caused cost, maintenance cost, repair cost and design review cost. Let *Cost* represent the safety-related life cycle cost function. *Cost* is given by:

$$\min : Cost = COST_T^* + COST_M^* + COST_R^* + COST_D^*$$

subject to: $MTBM_{max} \geq MTBM \geq MTBM_{min}$

$$0 \leq \Delta P_{Dj} \leq P_{Dj}(\text{MTBM}) \; (j = 1, 2, ..., c).$$

The first three terms of the cost model deal with the maintenance policies and the last term takes into account both the maintenance policies and design review actions. This model implies that the maintenance policies and the design review actions should be implemented to minimise the safety-related life cycle cost.

4 BICRITERIA MODELS FOR TECHNO-ECONOMIC ANALYSIS

4.1 A techno-economic modelling

A techno-economic model is proposed which combines the safety model with the economic model. Let X = MTBM, $y_j = \Delta_{Dj}$ (j = 1, 2,..., c) and $Y = [y_1, y_2, ..., y_c]^T$. Since $COST_T^*$ $COST_M^*$ and $COST_R^*$ are functions of X, and $COST_D^*$ is a function of X and Y, such a techno-economic model is given by:

$$\min : Cost = COST_T^*(X) + COST_M^*(X) + COST_R^*(X) + COST_D^*(X, Y)$$

$$\min : Risk = [\sum_{i=1}^{n} K_i \times P_i(X) + \sum_{j=1}^{c} K_{Dj} \times (P_{Dj}(X) - y_i)]$$

subject to: $X_{max} \geq X \geq X_{min}$

$$0 \leq y_i \leq P_{Dj}(X) \; (j = 1, 2, ..., c).$$

X and Y are design variables which need to be determined to attain the cost and risk objectives as closely as possible.

Safety should be carefully considered to minimise the potential risks at the initial design stages. After the system process diagram has been constructed and safety analysis has been conducted using the safety analysis approach described in Section 2, the above described techno-economic model can be formulated in order to improve the design aspects and maintenance policies.

As described early, *Cost* and *Risk* are two competing objectives. The purpose of design synthesis is therefore to evolve compromise design solutions by balancing and

effectively utilising resources so that these two objectives can be simultaneously attained as closely as possible.

4.2 Problem transformation and optimisation

The probability distributions $P_i(X)$ and $P_{Dj}(X)$ ($i = 1, 2,..., n$; $j = 1, 2,..., c$) and the failure distributions $f_i(X)$ ($i = 1, 2,..., m$) are, generally, not known explicitly. At a specific X, however, the values of these distributions can be obtained using the bottom-up safety analysis approach described early. If the safety analysis is conducted at a sufficient number of discrete values of X, the values of these distributions at any X with $X_{max} \geq X \geq X_{min}$ may then be predicted using the linear interpolation, resulting in piecewise linear distribution functions.

The piecewise linear probability function $P_i(X)$ of the top event T_i can be represented as follows:[20]

$$P_i(X) = \sum_{j=1}^{N-1} \alpha_{Pi,j}|X - X^j| + \beta_{Pi}X + \gamma_{Pi} \quad i = 1, 2, ..., n \tag{1}$$

where: N = the number of the sections of $P_i(X)$. X^j is a sampled value of X ($j = 0, 1,..., N$).

$$\alpha_{Pi,j} = \frac{1}{2}(t_{Pi,j+1} - t_{Pi,j}), \beta_{Pi} = \frac{1}{2}(t_{Pi,1} + t_{Pi,N}), \gamma_{Pi,j} = \frac{1}{2}(S_{Pi,1} + S_{Pi,N}). \tag{2}$$

$t_{Pi,j}$ is the slope of the jth section and $s_{Pi,j}$ is the y-intercept for the jth section of the probability function $P_i(X)$, starting from X^{j-1} and being terminated at X^j, that is

$$t_{Pi,j} = \frac{P_i(X^j) - P_i(X^{j-1})}{X^j - X^{j-1}} \tag{3}$$

$$s_{Pi,1} = P_i(X^0) - t_{Pi,1}X^0 \quad s_{Pi,N} = P_i(X^N) - t_{Pi,N}X^N. \tag{4}$$

If the following auxiliary variables a_j^+ and a_j^- are introduced,

$$a_j^+ = \frac{1}{2}\{|X - X^j| + (X - X^j)\} \text{ and } a_j^- = \frac{1}{2}\{|X - X^j| - (X - X^j)\} \tag{5}$$

then the probability function $P_i(X)$ can be represented by:[20]

$$P_i(X) = \sum_{j=1}^{N-1} \alpha_{Pi,j}(a_j^+ + a_j^-) + \beta_{Pi}X + \gamma_{Pi}, i = 1, 2, ..., n \tag{6}$$

under the restrictions

$$a_j^+ - a_j^- = X - X^j;$$

$$a_j^+ \times a_j^- = 0; \; a_j^+, a_j^- \geq 0, \; j = 1, 2, ..., n. \tag{7}$$

Similarly, the subsystem failure functions $f_i(X)$ can be represented as follows:

$$f_i(X) = \sum_{j=1}^{N-1} \alpha_{fi,j}(a_j^+ + a_j^-) + \beta_{fi}X + \gamma_{fi}, \; i = 1, 2, ..., m \tag{8}$$

where:

$$\alpha_{fi,j} = \frac{1}{2}(t_{fi,j+1} - t_{fi,j}), \beta_{fi} = \frac{1}{2}(t_{fi,1} + t_{fi,N}) \text{ and } \gamma_{fi} = \frac{1}{2}(s_{fi,1} + s_{fi,N}) \tag{9}$$

$$t_{fi,j} = \frac{f_i(X^j) - f_i(X^{j-1})}{X^j - X^{j-1}} \tag{10}$$

$$s_{fi,1} = f_i(X^0) - t_{fi,1}X^0; \; s_{fi,N} = f_i(X^N) - t_{fi,N}X^N \tag{11}$$

$P_{Di}(X)$ can also be represented as follows:

$$P_{Di}(X) = \sum_{j=1}^{N-1} \alpha_{PDi,j}(a_j^+ + a_j^-) + \beta_{PDi}X + \gamma_{PDi}, \quad i = 1, 2, ..., c \tag{12}$$

where: $\alpha_{PDi,j} = \frac{1}{2}(t_{PDi,j+1} - t_{PDi,j}), \beta_{PDi} = \frac{1}{2}(t_{PDi,1} + t_{PDi,N})$ and $\gamma_{PDi} = \frac{1}{2}(s_{PDi,1} + s_{PDi,N})$ (13)

$$t_{PDi,j} = \frac{P_{Di}(X^j) - P_{Dj}(X^{j-1})}{X^j - X^{j-1}} \tag{14}$$

$$s_{PDi,1} = P_{Di}(X^0) - t_{PDi,1}X^0; \; s_{PDi,N} = P_{Di}(X^N) - t_{PDi,N}X^N. \tag{15}$$

The bicriteria problem for optimising both risk and cost objectives may then be transformed as follows:

$$GP \begin{cases} \min Cost = \sum_{i=1}^{n} (C_{Ti} + C_{Li} + C_{Ri} - COST_0 \times BT_{Ti})P_i(X) \\ \qquad + (C_{MLi} + C_{MPi} + C_{MMi} - COST_0 \times BT_{Mi})\frac{T_{PT}}{X} \\ \qquad + \sum_{i=1}^{m} (C_{RLi} + C_{RPi} + C_{RRi} - COST_0 \times BT_{Ri})f_i(X) \\ \qquad + \sum_{i=1}^{c} (\frac{M_i}{P_{Di}(X)} - C_{Di} - COST_0 \times BT_{Di})y_i \\ \min Risk = \sum_{i=1}^{n} K_i \times P_i(X) + \sum_{j=1}^{c} (K_{Dj} \times P_{Dj}(X) - y_i)^T \\ s.t. \quad X_{\min} \leq X \leq X_{max} \qquad Y = [y_1, y_2, ..., y_c] \\ o \leq y_i \leq P_{Di}(X) \qquad i = 1, ..., c \\ X - a_j^+ + a_j^- = X^j \qquad j = 1, ..., N-1 \\ a_j^+ \times a_j^- = 0; \; a_j^+, a_j^- \leq 0 \qquad j = 1, ..., N-1 \end{cases} \tag{16}$$

The GP as defined in eqn (16) can be used to obtain compromise designs and to find the interaction between cost and risk. In eqn (16), $P_i(X)$, $f_i(X)$ and $P_{Di}(X)$ are represented by eqns (6), (8) and (12), respectively. GP is a nonlinear bicriteria programming problem, which can be solved using the existing MODM techniques.[13,19,20]

Let $V = [X, a_1^+, a_1^-, ..., a_{N-1}^+, a_{N-1}^-, y_1, ..., y_c]$. V is referred to as a design vector. The problem as represented by eqn (16) is then to search for designs that can attain the two objectives as closely as possible. There is generally no single design vector available which could simultaneously minimise the cost and risk objectives. It is therefore significant to search for non-dominated (or efficient) design vectors for evaluation.[19] In the next section, an example will be used to demonstrate how to generate such efficient designs.

5 AN EXAMPLE

The hydraulic hoisting transmission system of a marine crane is functionally shown in Fig. 2. This system is used to control the crane motions such as hoisting up or hoisting down loads as required by the operator.[17,18] It consists of five subsystems, namely an hydraulic oil tank, an auxiliary system, a control system, a prevention system and an hydraulic servo transmission system. Each subsystem is associated with several failure modes.[9,18] An occurrence of each failure mode associated with each subsystem may result in possible consequences, with the diverse severity class depending on the nature of the failure mode and the interactions of the subsystems.

1. The following assumptions are made for the convenience of analysis:
2. All the subsystems return to their original conditions after a full maintenance.
3. Every subsystem is considered to be independent.
4. Failed subsystems are repaired 'same as new' and the rest of the subsystems are not affected by the repairs.

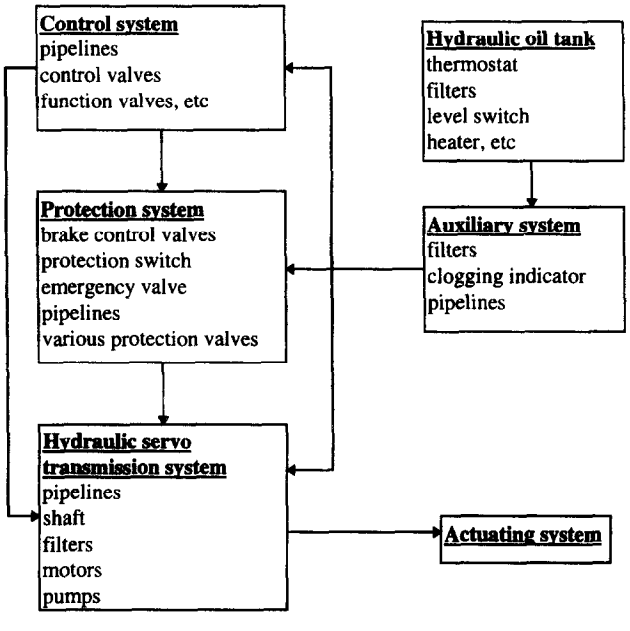

Fig. 2. The diagram of an hydraulic hoisting transmission system of an offshore crane.

The failure modes of the subsystems with severity class 4 are not taken into account for the study of the system top events, and the failure modes of the subsystems with severity classes 3 and 4 would not cause the system to shut down.

5.1 Top event-caused cost

The system top events and the associated causes of the hydraulic hoisting transmission system can be identified using the inductive bottom-up safety analysis approach described in Section 2. After the Boolean representation table of each subsystem has been constructed by making use of the information produced using FMECA, the final Boolean representation table of this system can be constructed by studying the subsystem interrelations and applying the rules of elimination and simplification.[17,18] Each row in the final system Boolean representation table represents a possible condition for an occurrence of the system's output state. For example, if '*the output of the control system cannot be closed for lowering motion*' and '*shaft failure of the hydraulic servo transmission system*' simultaneously occur, the top event '*hoisting down continuously not as required*' will happen.[17,18]

The system top events are identified as follows from the constructed final system Boolean representation table:[18]

T_1: Hoisting down continuously not as required.
T_2: Hoisting up continuously not as required.
T_3: No output from the package output motor.

10 cut set are identified which are associated with T_1, 43 cut sets with T_2 and 14 cut sets with T_3.[17,18] The possible consequences resulting from the three identified system top events are described as follows:[17,18]

T_1: Possibility of damage to the boom, ranging from minor distortion to total collapse (buckling). Possible rupture of the hoisting rope resulting in a dropped load. A dropped load may result in a total destruction of the lifted load, damage to the surrounding structure and other goods within the operating radius and possible death or severe injury to personnel.
T_2: A dropped load resulting in the probable consequences described in T_1.

Table 1. The probabilities of occurrence of T_1, T_2 and T_3

MTBM(hr)	T_1	T_2	T_3
1000	0.0775	0.0001	0.0222
2000	0.0775	0.0002	0.0250
4000	0.0776	0.0012	0.0275
6000	0.0792	0.0026	0.0288
8000	0.0792	0.0075	0.0336
10000	0.0803	0.0140	0.0366
12000	0.0810	0.0227	0.0374
14000	0.0815	0.0312	0.0494
16000	0.0830	0.0433	0.0498
18000	0.0899	0.0514	0.0504
20000	0.0929	0.0670	0.0638

Table 2. The parameters in the top event-caused cost model

C_T	pounds	C_L	pounds	C_R	pounds
C_{T1}	200000	C_{L1}	10000	C_{R1}	10000
C_{T2}	600000	C_{L2}	20000	C_{R2}	20000
C_{T3}	100000	C_{L3}	5000	C_{R3}	5000

T_3: A dropped load resulting in the probable consequences described in T_1.

The probabilistic assessment of the top events can be carried out on the basis of the obtained final system Boolean representation table. Given the failure data of the basic events associated with T_1, T_2 and T_3, the probability of occurrence of each top event with MTBM can be calculated using the Monte Carlo simulation method[16,17] and shown in Table 1. (See also Fig. 3.)

In the top event-caused cost model, n is equal to 3, and other parameters are shown in Table 2.

5.2 Maintenance cost

The parameters in the maintenance cost model are shown as follows: $C_{ML1}+C_{MP1}$ = 4000 pounds; C_{MM1} = 500 pounds; T_{PT} = 20 x 365 x 24 hr.

5.3 Repair cost

When studying a basic event failure, an exponential distribution in which the failure rate is constant is usually used to describe it. This is because the constant failure rate is a characteristic of a basic event.[14] The probability of occurrence of a basic event failure following an exponential distribution can be obtained by

$$P(t) = 1 - e^{-\lambda t}$$

where t is the period of time of interest.

The exponential distribution is the most widely used distribution in application and it is also the most simple to deal with.[14] Therefore, in this paper, it is assumed that each basic event failure of a subsystem, which is independent of others as discussed earlier, follows an exponential distribution. After the failure data of such basic events has been obtained from the FMECA, the discrete values of failure distributions (i.e., the distributions of the numbers of failures) of the subsystems can be produced as shown in Table 3 using the Monte Carlo simulation method.[16,17] (See also Fig. 4.)

In the repair cost model, m is equal to 4 and other parameters are shown in Table 4.

5.4 Design review cost

The probabilities of occurrence of the cut sets associated with the system top events T_1, T_2 and T_3 with respect to MTBM can be calculated using the Monte Carlo simulation method, on the basis of the obtained system Boolean representation table.[16,17] If six cut sets with the highest probabilities of occurrence with respect to each MTBM value are taken into account, the total eight cut sets regarding all MTBM values are identified for reduction or elimination. This is because the probabilities of occurrence of the cut sets change with MTBM and therefore the six cut sets with the highest probabilities of occurrence may not be the same for

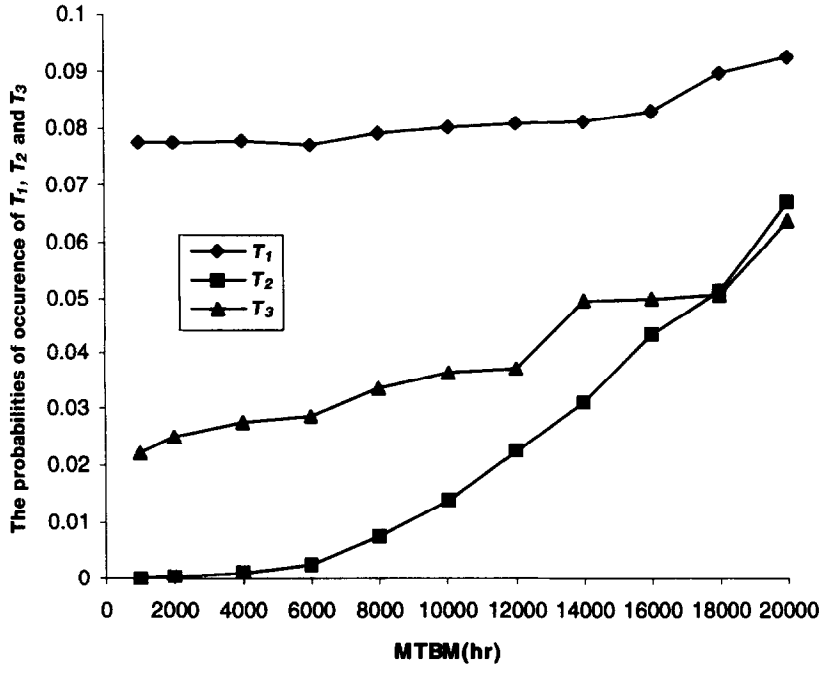

Fig. 3. Failure distributions of T_1, T_2 and T_3 with MTBM.

Table 3. The discrete values of failure distributions of the subsystems

MTBM	Sub-system	$f_i(X)$	MTBM	Sub-system	$f_i(X)$
1000	control	$f_1 = 0.0428$	2000	control	$f_1 = 0.0504$
	protection	$f_2 = 0.4474$		protection	$f_2 = 0.5188$
	servo	$f_3 = 0.6656$		servo	$f_3 = 0.7922$
	oil tank	$f_4 = 0.0398$		oil tank	$f_4 = 0.0500$
4000	control	$f_1 = 0.0700$	6000	control	$f_1 = 0.0824$
	protection	$f_2 = 0.6758$		protection	$f_2 = 0.8078$
	servo	$f_3 = 1.0054$		servo	$f_3 = 1.2692$
	oil tank	$f_4 = 0.0644$		oil tank	$f_4 = 0.0774$
8000	control	$f_1 = 0.0990$	10000	control	$f_1 = 0.1134$
	protection	$f_2 = 0.9858$		protection	$f_2 = 1.1244$
	servo	$f_3 = 1.4958$		servo	$f_3 = 1.7092$
	oil tank	$f_4 = 0.0846$		oil tank	$f_4 = 0.1024$
12000	control	$f_1 = 0.1364$	14000	control	$f_1 = 0.1480$
	protection	$f_2 = 1.3004$		protection	$f_2 = 1.4398$
	servo	$f_3 = 1.9486$		servo	$f_3 = 2.1734$
	oil tank	$f_4 = 0.1188$		oil tank	$f_4 = 0.1278$
16000	control	$f_1 = 0.1610$	18000	control	$f_1 = 0.1820$
	protection	$f_2 = 1.5866$		protection	$f_2 = 1.7176$
	servo	$f_3 = 2.4022$		servo	$f_3 = 2.6664$
	oil tank	$f_4 = 0.1356$		oil tank	$f_4 = 0.1492$
20000	control	$f_1 = 0.1916$	20000	control	$f_1 = 0.1916$
	protection	$f_2 = 1.9128$		protection	$f_2 = 1.9128$
	servo	$f_3 = 2.8956$		servo	$f_3 = 2.8956$
	oil tank	$f_4 = 0.1684$		oil tank	$f_4 = 0.1684$

Table 4. The parameters in the repair cost model

C_{RL}	pounds	C_{RP}	pounds	C_{RR}	pounds
C_{RL1}	1000	C_{RP1}	2000	C_{RR1}	2000
C_{RL2}	2000	C_{RP2}	4000	C_{RR2}	4000
C_{RL3}	2000	C_{RP3}	4000	C_{RR3}	4000
C_{RL4}	1000	C_{RP4}	2000	C_{RR4}	2000

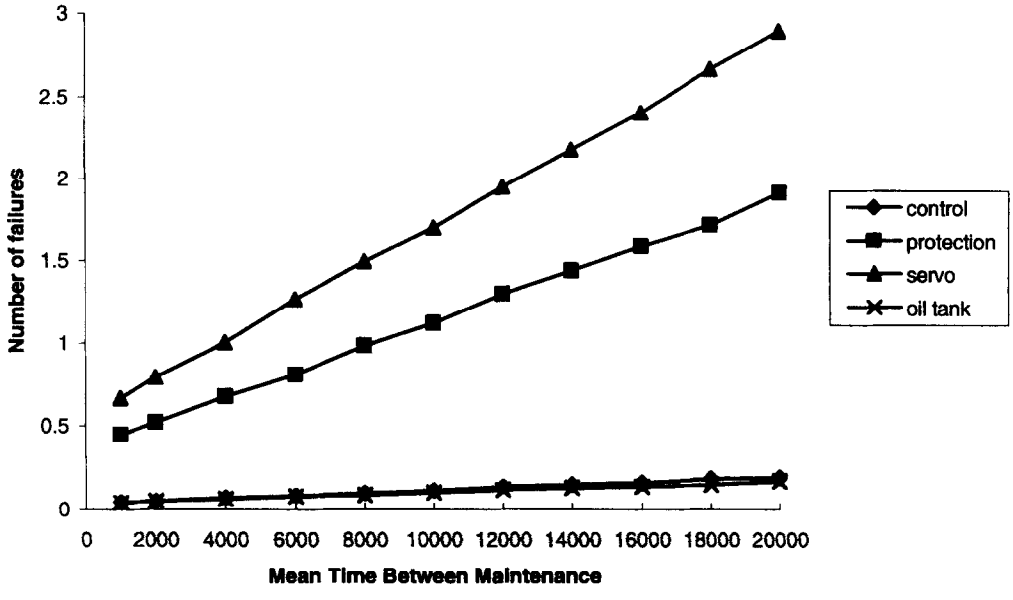

Fig. 4. Subsystem failure distributions with MTBM.

different MTBM values. These eight cut sets are described as follows:

Cut set 1: 'major leak in the hydraulic oil tank' *AND* 'level gauge failure of the hydraulic oil tank' *AND* 'major leak of the auxiliary system' *AND* 'the output form the control system cannot be closed for 'lowering' motion' *AND* 'major leak of the hydraulic servo transmission system'.

Cut set 2: 'major leak in the hydraulic oil tank' *AND* 'level gauge failure of the hydraulic oil tank' *AND* 'no output from the control pump of the auxiliary system' *AND* 'the output from the control system cannot be closed for 'lowering' motion' *AND* 'motor seizure of the hydraulic servo transmission system'.

Cut set 3: 'failure allowing contaminant into the auxiliary system' *AND* 'the output from the control system for hoisting up motion cannot be closed when required' *AND* 'failure of the switch when energised for the protection system' *AND* 'failure of the hoisting lower limit/slack rope prevention of the protection system'.

Cut set 4: 'the filter blocked for the auxiliary system' *AND* 'the blocking indicator of the auxiliary system fails to operate' *AND* 'major leak of the hydraulic servo transmission system'.

Cut set 5: 'the filter blocked for the auxiliary system' *AND* 'the blocking indicator of the auxiliary system fails to operate' *AND* 'no output from the package motor of the hydraulic servo transmission system'.

Cut set 6: 'the filter blocked for the auxiliary system' *AND* 'the blocking indicator of the auxiliary system fails to operate' *AND* 'pipe burst of the hydraulic servo transmission system'.

Cut set 7: 'the filter blocked for the auxiliary system' *AND* 'the blocking indicator of the auxiliary system fails to operate' *AND* 'short circuit of the hydraulic servo transmission system'.

Cut set 8: 'failure allowing contaminant into the auxiliary system' *AND* 'no major leak of the hydraulic oil tank' *AND* 'motor seizure of the hydraulic servo transmission system'

where the first two cut sets are associated with T_1, the third cut set with T_2 and the remainder with T_3.

For each MTBM value, the range of the probability reduction of occurrence of each cut set is shown in Table 5. (See also Fig. 5.)

In the design review cost model, c is equal to 8 and other parameters are shown as follows:

$C_{D1} = C_{D2} = C_{T1}+C_{L1}+C_{R1} = 220000$ pounds
$C_{D3} = C_{T2}+C_{L2}+C_{R2} = 640000$ pounds
$C_{D4} = C_{D5} = C_{D6} = C_{D7} = C_{D8} = C_{T3}+C_{L3}+C_{R3} = 110000$ pounds
$M_1 = M_2 = M_3 = M_4 = M_5 = M_6 = M_7 = M_8 = 8000$ pounds.

5.5 Operational cost

Assuming that the annual operational cost of this hydraulic hoisting transmission system is equal to 10000 pounds, the daily operational cost $COST_O$ can be obtained by: $COST_O = 10000/365$ pounds.

The parameters for the modification of the models of the top event-caused cost, repair cost, maintenance cost and design review cost are shown in Table 6, where $i = 1, 2, ..., T_{PT}/X$.

5.6 Optimisation results

Other parameters in the techno-economic model are shown as follows: $K_{D1} = K_{D2} = K_{D4} = K_{D5} = K_{D6} = K_{D7} = K_{D8} = K_1 = K_3 = 1$, $K_{D3} = K2 = 2$, $X_{min} = 1000$ hr, $X_{max} = 20000$ hr.

The non-linear *GP* shown in eqn (16) can be solved using the software for multiple objective non-linear programming.[13,19,20] The optimisation results are shown in Fig. 6 and discussed as follows:

If only the cost objective is optimised, the minimum *Cost* is equal to 121631 pounds and the design is located at point 2 as shown in Fig. 6. In this case, the risk objective is equal to 0.32, X or MTBM is equal to 18000 hr, and cut sets 1 and 3 are required to be eliminated. Elimination of such cut sets can be made by the use of more reliable components, the

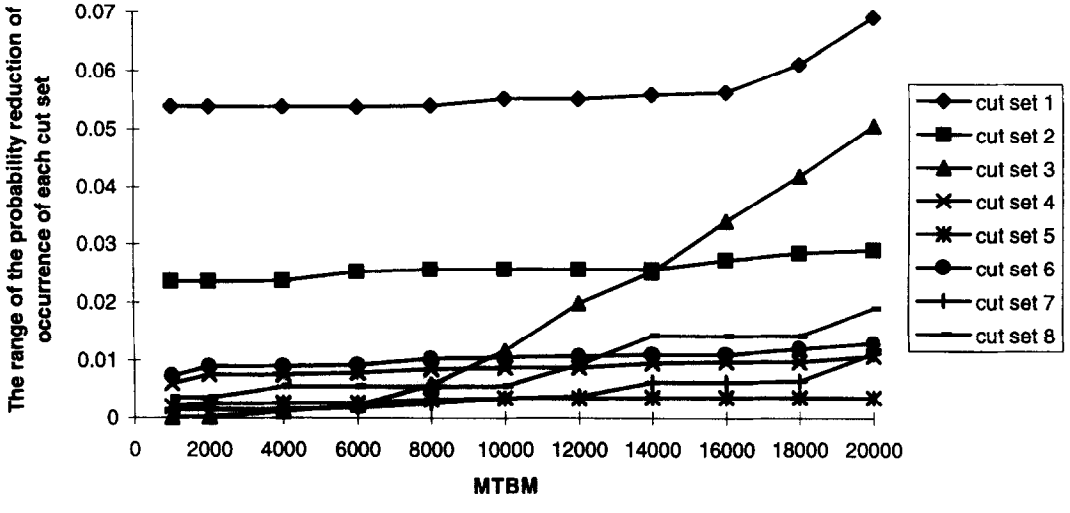

Fig. 5. The range of the probability reduction of occurrence of each cut set.

Table 5. The range of the probability reduction of occurrence of each cut set

MTBM(hr)	Cut sets							
	1	2	3	4	5	6	7	8
1000	0.0539	0.0236	0.0001	0.0060	0.0020	0.0074	0.0014	0.0036
2000	0.0539	0.0236	0.0002	0.0076	0.0026	0.0090	0.0014	0.0036
4000	0.0539	0.0237	0.0011	0.0076	0.0026	0.0090	0.0014	0.0054
6000	0.0539	0.0253	0.0022	0.0079	0.0026	0.0092	0.0018	0.0054
8000	0.0541	0.0257	0.0058	0.0086	0.0032	0.0104	0.0026	0.0054
10000	0.0553	0.0257	0.0117	0.0088	0.0034	0.0106	0.0034	0.0056
12000	0.0553	0.0257	0.0199	0.0088	0.0034	0.0108	0.0038	0.0094
14000	0.0560	0.0257	0.0253	0.0096	0.0036	0.0110	0.0062	0.0142
16000	0.0564	0.0274	0.0340	0.0098	0.0036	0.0110	0.0062	0.0142
18000	0.0613	0.0286	0.0419	0.0098	0.0036	0.0120	0.0064	0.0142
20000	0.0693	0.0292	0.0507	0.0108	0.0036	0.0130	0.0112	0.0190

provision of protection systems, sensors and alarming systems, or a combinations of them, as described previously. The detailed study in this area is outside the range of this paper.

If only the risk objective is minimised, the minimum *Risk* is equal to 0.10 and the design is located at point 1. In this case, the cost objective is equal to 839600 pounds, X is equal to 1000 hr, and cut sets 1, 2, 3, 4, 5, 6, 7 and 8 are all required to be eliminated.

Each point in the curve shown in Fig. 6 is an efficient design regarding both cost and risk objectives. A design is efficient or Pareto optimal if it is not dominated by any other feasible designs in terms of the two objectives. At point 5, for example, the cost and risk objectives are equal to 262364 pounds and 0.1082, respectively, X is equal to 4241 hr, and all eight cut sets are required to be eliminated. There is no other design available which could have the *Cost* and *Risk* values lower than 262364 pounds and 0.1082 simultaneously. At point 6, the cost and risk objectives are equal to 139516 pounds and 0.1696, respectively, X is equal to 10000 hr, and cut sets 1, 2, 3 and 6 are required to be eliminated.

The ideal design is located at point 3 where both the cost and risk objectives are simultaneously minimised. However, such a design is not feasible. Therefore, only compromise designs can be obtained. The best compromise design is located at a point in the frontier, which is nearest to the ideal design point.

If the risk and cost objectives are of equal importance, such a best compromise design (i.e., point 4) can be obtained using minimax approach.[13,20] At point 4, *Cost* and *Risk* are equal to 193020 pounds and 0.1198, respectively, X is equal to 6269 hr, and cut sets 1, 2, 3, 4, 6 and 8 are required to be eliminated.

It can be noted, from Fig. 6, that *Cost* is significantly reduced with a slight increase of *Risk* from point 1 to point 5 in the efficient frontier, and that *Risk* is significantly reduced with a slight increase of *Cost* from point 2 to point 6. These two sections should obviously be avoided in the design. A practical efficient design can be at some point in the section between 5 and 6, depending on the particular requirements on cost and safety to be considered. For instance, if safety is a comparatively important factor, an efficient design may be chosen from the section between points 5 and 4; and if cost is a comparatively important factor, an efficient design may be chosen from the curve between points 4 and 6. Each point corresponds to a fixed design vector V.

From the above analysis, it is obvious that the optimisation results can assist the designer in understanding the problem and making a decision as to what maintenance policies and design review actions should be taken.

6 CONCLUDING REMARKS

Based on safety analysis, a techno-economic modelling methodology is proposed in this paper to incorporate safety into the design process from the initial stages and to make design decisions. In this methodology, the safety parameters are obtained using an inductive bottom-up safety analysis approach. This gives a higher level of confidence that all system top events and the associated cut sets are identified. A techno-economic model can be constructed by utilising the safety information produced. MODM techniques can be applied to deal with the obtained bicriteria optimisation model. Such a techno-economic modelling methodology provides the safety analyst with a rational tool to make

Table 6. The parameters for the modification of the models

BT_{R1}	2	BT_{T1}	5	$BT_{D1} = BT_{T1} = 5$	$BT_{D5} = BT_{T3} = 5$
BT_{R2}	1	BT_{T2}	5	$BT_{D2} = BT_{T2} = 5$	$BT_{D6} = BT_{T3} = 5$
BT_{R3}	2	BT_{T3}	5	$BT_{D3} = BT_{T2} = 5$	$BT_{D7} = BT_{T3} = 5$
BT_{R4}	1	BT_{Mi}	5	$BT_{D4} = BT_{T3} = 5$	$BT_{D8} = BT_{T3} = 5$

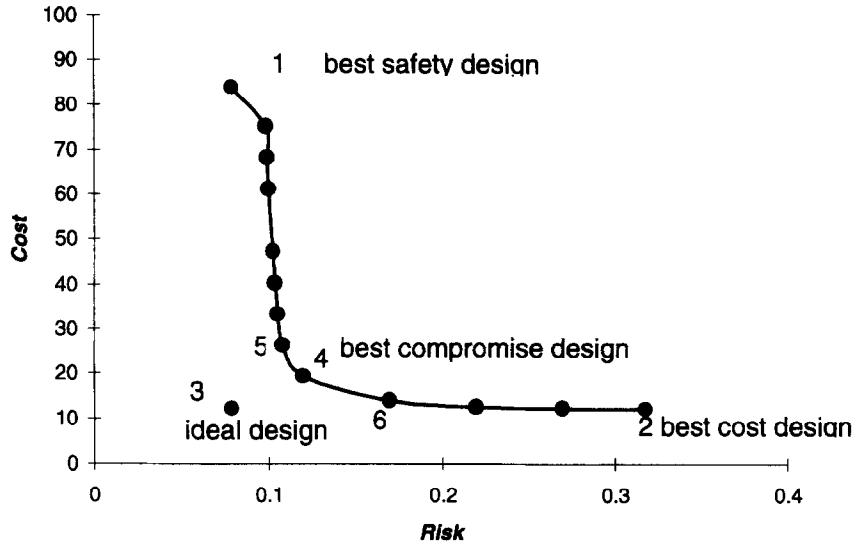

Fig. 6. The optimisation results.

full use of the information produced in safety analysis and to take into consideration both design aspects and maintenance policies simultaneously.

From the illustrative example, it is noted that there exist two competing demands of safety and economy. The decision as to which one is to be stressed may be dependent on the particular situation in hand. The proposed techno-economic modelling methodology can be used to assist designers in understanding the interaction between safety and economic considerations, so as to balance and best utilise resources for design of a large marine or offshore engineering product.

The safety information used in this paper is produced on the basis of the final system Boolean representation table. It is obviously also possible to generate such information on the basis of the cut sets associated with system top events produced using PRA approaches such as FTA.

ACKNOWLEDGEMENTS

The authors are indebted to the UK Science and Engineering Research Council for providing the financial support under Grant No. GRF 95306.

REFERENCES

1. Carpenter, S. J. & Fleming, J. M. An integrated approach to the safety assessment of offshore production facilities. In *SPE Asia-Pacific Conference*, Perth, Western Australia, 4–7 November 1991, pp. 693–704.
2. Department of Energy, *The public inquiry into the Piper Alpha disaster*, (Cullen Report), HMSO, London, UK, 1990.
3. Goss, R., Rational approach to maritime safety. *Trans. NE Inst. Engineers and Ship Builders*, **105** (1989) 97–110.
4. Henley, E.J. & Kumamoto, H., *Probabilistic risk assessment*, IEEE Press, New York, 1992.
5. House of Lords, Safety aspects of ship design and technology. Select Committee on Science and Technology, 2nd Report, *HL Paper 30-I*, London, UK, 1992.
6. Kriger, G. & Piermattei, E., Risk analysis applied to offshore platforms during the unpiled installation phase. In *15th Annual OTC*, Houston, Texas, May 1983, pp. 9–17.
7. McNichols, G.R., Cost-risk procedures for weapon system risk analysis. In *Proc. Ann. Reliab. Maint. Symp.*, IEEE Press, 1981, pp. 86–94.
8. Procedures for performing a failure mode, effects and criticality analysis. Military Standard, *MIL-STD-1629A*, Naval Ship Engineering Center, Washington DC.
9. FMECA of NEI pedestal crane. *Report No. NECL01*, National Engineering Laboratory, Glasgow, 1987.
10. Rasmussen, M., Lower maintenance cost through maintenance optimisation in design and operation. *Paper 5, ICMES 90*, Marine Management (Holdings) Ltd, London, 1990, pp. 53–58.
11. Ruxton, T. & Wang, J., Advances in marine safety technology applied to marine engineering systems. In *Proc. First Joint Conference on Marine Safety and Environment*, Delft, The Netherlands, 1–5 June 1992, pp. 421–432.
12. Sen, P., Labrie, C.R., Wang, J., Ruxton, T. & Chan, J., A general design for safety framework for large Made-To-Order engineering products. In *First Newcastle Int. Conf. Quality and Its Applications*, Newcastle, UK, 1–3 September 1993, pp. 99–505.
13. Sen, P, & Yang, J.B., A multiple criteria decision support environment for engineering design. In *Proc. 9th Int. Conf. Engng Design*, Hague, The Netherlands, 17–19 August 1993, pp. 465–472.
14. Vinogradov, O., *Introduction to mechanical reliability, a designer's approach*, Hemisphere Publishing Corporation, NY, 1991.
15. Wang, J. & Ruxton, T., *Design for safety of Made-To-Order (MTO) products'*, ASME Publication 93-DE-1, New York, 1993, pp. 1–12.
16. Wang, J., Labrie, C.R. & Ruxton, T., Computer simulation techniques applied to the prediction and control of safety in maritime engineering. *Inst. Marine Engineers Trans. C*, **105** (1993) 21–34.
17. Wang, J., Formal safety analysis methods and their application to the

design process. Ph.D. thesis, Engineering Design Centre, University of Newcastle upon Tyne, 1994.

18. Wang, J., Ruxton, T. & Labrie, C.R., Design for safety of the engineering systems with multiple failure state variables. *Engineering Reliability and System Safety*, **50** (1995) 271–284.
19. Yang, J.B., Chen, C. & Zhang, Z.J., The interactive step trade-off method (ISTM) for multiobjective optimization. *IEEE Trans. Systems, Man, & Cybernetics*, **20** (1990) 688–695.
20. Yang, J. B. & Sen, P., An interactive MODM method for design synthesis with assessment and optimization of local utility functions. *Eur. J. Oper. Res.*, 1996 (in press).