A Method of Alarm System Analysis in Process Plants With the Aid of an Expert Computer System

by

M. Modarres and T. Cadman
A METHOD OF ALARM SYSTEM
ANALYSIS IN PROCESS PLANTS
WITH THE AID OF AN EXPERT COMPUTER SYSTEM

M. Modarres
T. Cadman

Department of Chemical and Nuclear Engineering
The University of Maryland
College Park, Maryland 20742

Presented for Publication to
Computers & Chemical Engineering Journal
(September, 1985)
A METHOD OF ALARM SYSTEM
ANALYSIS IN PROCESS PLANTS
WITH THE AID OF AN EXPERT COMPUTER SYSTEM

M. Modarres
T. Cadman
Department of Chemical and Nuclear Engineering
The University of Maryland
College Park, Maryland, 20742

ABSTRACT:
Design and improvement of alarm systems in process plants has been given considerable attention recently. A methodology is presented in this paper which can be used as an aid in the design of new alarm systems or in the improvement of existing alarm systems. The methodology is incorporated in a computer software into which expert knowledge of a given process plant can be entered and used to select a proper alarm system.
A METHOD OF ALARM SYSTEM
ANALYSIS IN PROCESS PLANTS
WITH THE AID OF AN EXPERT COMPUTER SYSTEM

M. Modarres
T. Cadman
Department of Chemical and Nuclear Engineering
The University of Maryland
College Park, Maryland 20742

SCOPE:

Alarm systems play a very important role in process plants. They aid the operator in his primary tasks of detecting and interrupting progression of a failure, and diagnosing and providing corrective actions for fault conditions. There are however, operator difficulties in handling alarms. A particular alarm system design can significantly affect the operators' success likelihood in receiving and processing alarms.

Several factors are important in the design or improvement of a given alarm system. Human likelihood of success using a given alarm system under a given fault condition is one obvious factor. Economical aspects of selecting alarm systems, given probable types and frequencies of fault conditions, should also be considered in the design or
improvement of alarm systems. A systematic approach is necessary to consider the effects of all these factors in evaluating a set of proposed alarm systems and in selecting the most appropriate alarm system. The purpose of this paper is to provide a method for determining the worth of a given alarm system by considering all factors which influence that worth.

In complex process plants, applications of the methodology presented in this paper can be very difficult without the aid of a computer. Therefore, a computer program is also described to carry out the methodology. Information regarding the process plant is entered into the program using the goal tree concept. The goal tree contains the expert knowledge of the process which in turn is used in the design or modification of the alarm system.
A METHOD OF ALARM SYSTEM
ANALYSIS IN PROCESS PLANTS
WITH THE AID OF AN EXPERT COMPUTER SYSTEM

M. Modarres
T. Cadman
Department of Chemical and Nuclear Engineering
The University of Maryland
College Park, Maryland 20742

CONCLUSIONS AND SIGNIFICANCE:

A methodology has been presented to perform systematic evaluation of alarm systems. The methodology is based on the goal tree concept through which process plants can be modeled. The process knowledge is represented in an expert system.

Goal trees are excellent tools for cause-consequence determination. The methodology makes use of decision trees which are constructed in parallel to goal trees to show all operator action(s) required to achieve each goal, and to show the consequences of operator's failure to achieve each goal. The decision trees can also model the progression of an initiating fault condition. The operator's likelihood of success to achieve each goal for a given alarm system design or alarm system modification can be estimated and used in the decision tree to estimate anticipated consequences.
of a given alarm design or modification. Anticipated consequence is defined as the probability of not achieving a goal, times the consequence of not achieving that goal. Finally, alarm system designs or modifications with a low anticipated consequence and low implementation cost can be identified for further evaluation as potential alarm systems for the process.

The methodology has been modeled in an expert system called UMPIRE-I in which process knowledge can be entered into the computer through a goal tree coupled with human success likelihoods. The rest of the analysis is performed by UMPIRE-I. The code is user friendly and can be used with minimal training. An example is also provided in the paper to further clarify the methodology.

This method has been applied to several limited scale engineering processes with rather significant success.
1. Introduction

The understanding and processing of hardware failures in a large process plant is a complex task for the operators of these plants. Although most of the large process plants are automatically controlled by a process computer, in case of major hardware failure, the control system generates alarm signals for operator control. The plant operator must administer the corrective action based upon the information provided by the control system in order to safely cope with the fault condition. It is very important to provide the operator with a set of adequate information for the effective diagnosis and administration of the fault condition.

The purpose of this paper is to present a methodology for determining a cost justified method of determining required alarms in a process plant. The methodology is automated in an expert system computer package. The methodology is based on the goal tree approach [1], which has been recently used for various safety analyses in nuclear power plants. The goal tree provides the basis of the knowledge structure of the developed expert system.

Goal trees can completely and rigorously describe a process plant and its operations. Goal trees incorporate a structured approach that shows how an objective in a plant is achieved. This is done by defining an objective and partitioning it into a series of related sub-objectives or goals; these goals in turn are broken down into subgoals.
or functions. The partitioning continues until the description of a function cannot be made without referring to hardware. At this point, the success path(s) of hardware operation is displayed. The operator plays a key role in actively switching over or turning off success path(s) of the hardware. This is done when operators keep the plant running while dealing with safety situations as described by Lees [2]. In this role the operator can only affect the timing of an operation. For example, the impact of hardware failure can be minimized by the operator's determining how to accomplish a required plant function by using hardware other than that which failed. The use of adequate and sufficient levels of alarms can significantly influence the operator's ability to properly order the timing of an operation.

Operators also have a second role in which they act as an intelligent support system; analyzing information and developing strategies to improve the quality of hardware performance. In this role, the operator interrupts the progression of a small component failure into a major hardware failure. The methodology and expert system presented in this paper are equally applicable to designing or improving alarms that influence both of the noted operator roles.

The technique developed within this methodology provides the kind of in-depth understanding that leads to useful alternatives for improving the ability of the operators to cope with potential faults in a process plant. The methodology identifies human interfaces with hardware which
affect the probability of successful achievement of a function and the objective. Further, it provides a means of assessing the extent to which each human/hardware interface contributes to the achievement of an objective under a particular plant condition and a particular alarm system. It provides the means to:

. Evaluate improvements for a given or postulated design change to an alarm system.
. Compare the economic benefit that would arise from improved performance with the expected cost of installing the alarm system being included in the analysis.

An exhaustive review of the state of the art alarm system analysis is given by Lees [2].

2. Development of A Goal Tree

A goal tree is typically displayed in tree format so that the interrelationships of the goal tree objective and its supporting goals can be clearly represented and easily recognized [3-7].

The first step in development of the tree involves definition of the top goal or objective. This top goal must be explicitly defined in terms which make it a single unambiguous statement. It is from this definition that the analyst will identify and relate all the different plant goals and subgoals which must be achieved to attain the overall objective.

The goal tree is built vertically downward from the
objective in levels, wherein the analyst subsequently decomposes each identified goal into a necessary and sufficient set of dependent subgoals. As the vertical detailed development of the tree increases, it is necessary that tests be applied to ensure its accuracy and completeness, and that the proper hierarchy between goals and subgoals be rigorously maintained. This latter requirement is critical if the tree is to be capable of providing the needed framework for cause-consequence analyses such as the analysis of a given alarm system.

The tests which are to be applied at every level of the tree to ensure adequacy are:

. Upon looking upward from any subgoal towards the objective or tree-top, it is possible to define explicitly why the specific goal or subgoal must be satisfied.

. Upon looking downward from any goal towards the bottom of the tree, it is possible to define explicitly how the specific goal or subgoal is satisfied.

Failure of the tree to pass either of these tests at any level implies that:

. there is a lack of completeness and that intermediate subgoals have been omitted, or

. the hierarchy of goals or their interdependencies have been neither rigorously nor completely defined.

The process of downward development of the tree continues until the analyst is unable to further define subgoals without reference to actual hardware. As soon as hardware
is explicitly mentioned, the tree become one which describes success paths, not goals.

It is important that this boundary between goals and success paths be recognized because this is the point at which the logic structure of the tree changes. Within the goal tree, all goals must be connected by logical AND gates, whereas the success paths must be connected to the goals they serve by logical OR gates. In this latter case, it should be recognized that a single input OR gate will be used if there is only one success path for any specific goal.

Use of the fact that all connectors in the goal tree are logical ANDs can be used to establish a convention which provides the analyst a means for easy distinction between the goal tree and the hardware success paths. The goal tree is drawn with no gates explicitly displayed. If a gate is shown, success paths are being described. Figure 1 illustrates the relationship of objective, goals, subgoals, and success paths.

An understanding of the logical structure of the tree is necessary to recognize that the nature of the goal tree does not in any way change the Boolean expression representing logical relationship of components to achieve the top goal for the plant, which is clearly a function of hardware configuration, not the individual goal structure. The implication of the above statements is that if the tree is to be used as an explicitly quantifiable analytic tool,
its structure below the goal level is the part which is critical.

The goal portion of the composite tree merely provides a visual display of the analyst's understanding of how the hardware interacts, and the effect of its performance on the plant objective. It is this understanding, or intelligence within the tree, which makes it so valuable in process plant design, improvement, and operation. Since it is possible to look at the composite goal/success-path tree and identify the exact relationship between any piece of hardware and the plant objective, the tree can become the desired cause-consequence framework so necessary for a comprehensive plant design, improvement or operation program. Through this mechanism it is possible, conceptually, to establish hardware performance requirements which in turn can be used to establish required alarm specification.

3. General Approach

The objective here is to present a methodology for determining the worth of alarms in a process plant. This is done by taking advantage of the cause-consequence nature of the developed goal tree for the defined plant objective to rank alternative alarm systems based on their economic consequence as well as their implementation cost.

To determine potential consequences of adopting a particular alarm system, the concept of a decision tree is used. The decision trees are pictorial representation
of all the operator actions necessary to achieve a goal and to stop the progression of a fault condition. These are binary trees in which one branch represents failure of the operator to act given a fault condition in the presence of a given set of alarms, and the other branch represents operator success. The decision trees are constructed in parallel to the goal tree. The decision trees initiate when all of the success paths of a given subgoal are lost. Decision trees have several decision points each relating to one of the subgoals of plant objective under analysis. Each decision point has two branches. One branch represents the achievement of the goal or subgoal (left branch) and the other represents the lack of achieving the goal or subgoal. One decision tree should be constructed parallel to each path of a goal tree. See Figure 2 for illustration of a typical decision tree which is parallel to one path of a goal tree.

Where the left branches of the decision tree terminates, the consequences of not achieving the respective subgoal is shown, for example in terms of potential casualties or temporary loss of plant operation. These consequences can always be converted to economic consequences. At each branch, given the state of the plant and plant alarms, the probability that operator could achieve the goal or subgoal by restoring the required success path(s) or stopping the progression of a fault condition must be determined.
This probability is highly influenced by the alarm system used.

Various human factors methods are available to determine the operator's probability of success under a given condition. The authors have applied the Success Likelihood Index Methodology (SLIM) [8,9] with a reasonable degree of success to determine human success probabilities. The basic rational of SLIM is that the likelihood of an error occurring in a particular situation depends on the combined effects of a relatively small set of Performance Shaping Factors (PSFs). The PSFs include both human traits (eg., competence, morale, motivation) and conditions of the work setting that are likely to influence an individual's performance. Some of the PSFs are highly influenced by alarms (eg., time available for an action, clarity of alarms, noise level). It is assumed that an expert judge (or group of judges) will be able to assess the relative importance, or weight, of each PSF with regard to its effect on the human success probability as well as the degree to which single PSF is actually significant during operation (ie, rate of a PSF). The weights and rates are then used to estimate human success probabilities [8].

For a proposed alarm design or modification, the associated goal tree is used in connection with the decision tree concept to determine the anticipated economic consequences of such an alarm system. For every path of the goal tree, a decision tree is constructed. The lowest level of each path ends with a subgoal that is supported by one or more
hardware success path(s). The frequency of losing all hardware success paths are estimated by using standard reliability methods and component failure data, including the probability of human operator action to prevent this loss (this probability is highly influenced by the amount and the way that alarms are presented to the operators). Similarly, the probabilities that the operator would achieve individual goals or subgoals in the goal tree path under analysis is estimated, and the economic consequences of not achieving each goal is determined. The anticipated consequences, for each branch of the decision tree of not achieving each subgoal is then determined using the estimated probabilities and economic consequences previously enumerated. The method of determining the anticipated consequences are discussed in the next section. The process is repeated for all of the paths of the goal tree, each having its own decision tree. The total anticipated consequence is then calculated by suming the individual anticipated consequences of each decision tree.

The process may be repeated for other proposed alarms to determine their anticipated consequences. The alarm system with the lowest anticipated consequence will be finally selected.

4. Formal Cost Consequence Analysis Using Goal Tree-Decision Tree Concept

Each proposed alarm modification or installation is analyzed to determine an estimated total cost of implementation.
This total cost includes the capital cost for equipment, the installation cost and the anticipated loss of revenue due to plant shut-down or plant capacity reduction required for installation and implementation. The total cost also includes other secondary costs such as those associated with administrative and related training activities required by the change.

The total cost can be determined by using the equation

\[ C^j_t = C^j_1 + C^j_2 + C^j_3 \]  \hspace{1cm} (1)

Where:
- \( C^j_1 \) is the capital cost of new equipment required for a proposed alarm system,
- \( C^j_2 \) is the installation cost including cost of labor and necessary plant shut-down time for a proposed alarm system,
- \( C^j_3 \) is the cost of institutional activities such as the cost of training required for proposed alarm system,
- \( C^j_t \) is the total cost associated with implementation of proposed alarm.

To determine the anticipated economic consequence
of a given alarm system consider one particular goal tree path as illustrated in Figure 2. Given initiator $i$ and successful operator intervention at decision point $j$, the anticipated consequence in this path, $R_{ij}$, is the product of the frequency of initiating fault condition $i$, the economic consequence given success at point $j$, the probability of operator success at point $j$, and the probability of operator failures at the lower decision points leading to point $j$. This is given by:

$$R_{ij} = f_i \prod_{k=1}^{j} k_j p_j (1 - p_k) \quad (2)$$

where:
- $f_i$ is the frequency of initiating event $i$
- $k_j$ is the economic consequence, given termination of failure progression at decision point $j$,
- $p_j$ is the conditional probability of operator's terminating the progression of the failure started by the initiating fault $i$ at decision point $j$ given an alarm system.

The total anticipated economic consequence of a given alarm system is then:

$$R = \sum_{i,j} R_{ij} \quad (3)$$

The values of cost and total anticipated economic consequence given by (1) and (3) can be used to determine the most appropriate alarm system.
One measure of the value of a proposed alarm system is the ratio of anticipated economic benefit to cost. A preliminary ranking of proposed alarm systems is therefore carried out based upon the anticipated economic consequence to cost ratio.

5. UMPIRE-I Expert System

An expert system of microcomputer programs called UMPIRE-I (University of Maryland Program for Information Requirement Evaluation) have been developed to perform the methodology discussed in this paper. The procedure used in UMPIRE-I may be conveniently summarized in four steps:

1. Reading the goal trees and enumerating the paths of the tree.

2. Specification of the economic consequence if the identified goals are not achieved.

3. Selection of an alarm system and calculation of the total anticipated economic consequence for the selected alarm system by inputting relevant human success probabilities at each decision point.

4. Comparison of the anticipated economic consequences computed using other alarm systems with the cost of implementing these alarm systems in order to identify the most economically significant alarm system.
Steps 1 and 2 are the data input steps of the procedure. For Step 1 an interactive, automatically prompted routine was used to enter the goal tree configuration for computational purposes. The routine begins with the identification of the top goal level of the tree and sequentially progresses down the tree. The program computes all paths which comprise the goal tree.

In step 2 for each goal, the economic consequence which would accompany the loss of that goal is specified (eg. in terms of dollars).

In Step 3 of the procedure, upon the selection of a hypothesized alarm system, the anticipated economic consequence is calculated, for the decision paths which comprise the goal tree. The operator's likelihood of success to achieve each goal given an alarm system is calculated separately by using SLIM-MAUD [8] and by entering into UMPIRE-I at this step. Equations (1) and (3) are then used to determine the total economic consequences.

The final step of the procedure used in this study is the comparison of the total anticipated economic consequences obtained by using alternate alarm systems with the cost of their implementation. The objective of the comparison is to identify the most economically significant alarm systems so that these alarm systems can be analyzed in further detail. The proposed alarm systems are then ranked and printed.
6. EXAMPLE

Consider the control of a large feed pump which is used to provide cooling water to a nitric acid process plant. Two different alarm systems are proposed for use in this plant, each has a different way of monitoring and controlling the pump.

In order to minimize pump failures which in turn helps to maximize the availability of this pump for operation, a goal tree is developed. The top objective of this tree is "Feed Pump Failure Prevented". All goals and subgoals associated with this objective are then identified by process engineers (experts). The completeness and hierarchy is maintained by strictly using the rules of constructing goal trees. Finally, those goals and subgoals that have a likelihood that their achievement can be enhanced through the aid of an alarm system are identified. Potential types of monitoring and alarming are then identified for applicable goals and subgoals. Figure 3 shows the goal tree. Two methods of monitoring and alarming are proposed. They are shown by alarm systems I and II in Figure 3 and the parameters measured by these two alarm systems are shown. The purpose of this example is to compare these two alarm systems.

Table 1 shows the likelihood of the operator's success to achieve a goal or subgoal for the two proposed alarm
systems, consequences of loosing the goal or subgoal and frequency of initiating a fault condition. These goals or subgoals without a consequence, an operator interaction or frequency of initiating fault condition are descriptive in nature. They are needed to keep the hierarchy within the tree and are not shown in Table 1. The operator probability of success is obtained by using the SLIM-MAUD [8] technique. In applying the SLIM-MAUD technique, experts were asked about their opinion of the values of weightings and ratings for each PSF that influences the success probability of operator's action (i.e., operator's action which results in achievement of a goal or subgoal under analysis). For the lowest level goals or subgoals where no operator interference is possible, but for which there is a certain frequency that they are not achieved (mostly due to parts failures), these frequencies are also noted in Table 1.

The goal tree in Figure 3 and the data in Table 1 are then entered into the UMPIRE-I program where a decision tree, paralleling the paths of the goal tree, is constructed. The decision tree only branches off at the goals and subgoals where the proposed alarm systems applies to aid operator in the required operator action. The consequences of not achieving the goals or subgoals by the operator are estimated by expert process engineers and entered into the UMPIRE-I Program. In Table 1 these consequences are shown as estimated hours of pump operation loss following the failure of the operator.
to achieve a goal or subgoal. The estimated consequences are based on prior repair experience in similar pumps.

A portion of UMPRIE-I output relating to one of the goal tree paths for the proposed alarm system I is shown in Figure 4. The same path is shown when alarm system II is applied. Similar types of calculations are repeated by the UMPRIE-I for all other paths of the goal tree shown in Figure 3 and for both of the proposed alarm systems. Anticipated consequences of each path are summed up to determine the total anticipated consequence (hours of lost pump operation in this example).

For this example, UMPRIE-I determined an anticipated lost pump operation of 0.0296 (hours per year) for alarm system I and 0.1363 (hours per year) for alarm system II. As expected, system I has less anticipated consequence since more parameters are measured, processed and provided to the operator. The use of more complex alarm systems would cost more in this case. A more rational economic decision can, however, be made by relating the anticipated consequence (eg, hours of lost pump operation ) to the anticipated economic consequence due to loss of plant productivity. The summation of the total cost of implementing each alarm system, and the anticipated economic consequence of the alarm system can be used for the effective selection of an alarm system. Since this example is primarily used for the purpose of demonstrating the methodology, a formal cost benefit analysis as stated above was not performed.
The results shown in this analysis is the effect of each proposed alarm system on the feed pump. The effect on the whole plant can potentially be significantly larger.

ACKNOWLEDGMENT

The authors wish to acknowledge the support of the University of Maryland's System Research Center during the course of the work described in this paper.
REFERENCES


5. R.N. Hunt, M. Modarres and M. L. Roush, Use of goal tree methodology to evaluate institutional practices and their effect on power plant hardware performance, Proceedings of the twelfth international reliability availability maintainability conference for the electric power industry, Baltimore, MD, April 1985.

REFERENCES (continued)

of the twelfth international reliability availability
maintainability conference for the electric power industry,
Baltimore, MD, April 1985.
7. M. Modarres, M.L. Roush and R.N. Hunt, Application
of goal trees for nuclear power plant hardware protection,
Proceedings of the eighth international conference
on structural mechanics in reactor technology, Brussels,
Belgium, August 1985.
8. D.E. Embrey, P.C. Humphreys, E.A. Rosa, B. Kirwan and
K. Rea, SLIM-MAUD: An approach to assessing human
error probabilities using structured expert judgement,
U.S. Nuclear Regulatory Commission, NUREG/CR-3518,
1984.
9. D.E. Embry, SLIM-SARA, success likelihood index methodology-
sensitivity analysis for the reliability assessment
<table>
<thead>
<tr>
<th>Function or Sub-function Description</th>
<th>Human Action Success Probability Alarm System II</th>
<th>Human Action Success Probability Alarm System I</th>
<th>Frequency of losing goal per year</th>
<th>Consequence of not achieving the goal (lost plant hour operation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oil Quality and Characteristics Nominal</td>
<td>-</td>
<td>-</td>
<td>0.1</td>
<td>-</td>
</tr>
<tr>
<td>Oil Temperature in Nominal Range</td>
<td>-</td>
<td>-</td>
<td>0.5</td>
<td>-</td>
</tr>
<tr>
<td>Rotor Dynamics</td>
<td>0.99</td>
<td>0.999</td>
<td>0.01</td>
<td>-</td>
</tr>
<tr>
<td>Rotor Balance</td>
<td>-</td>
<td>-</td>
<td>0.25</td>
<td>-</td>
</tr>
<tr>
<td>Coupled Loads</td>
<td>-</td>
<td>-</td>
<td>0.02</td>
<td>-</td>
</tr>
<tr>
<td>Rotor Electricity</td>
<td>0.9905</td>
<td>0.999</td>
<td>0.02</td>
<td>-</td>
</tr>
<tr>
<td>Bearing Dynamics</td>
<td>0.99</td>
<td>0.999</td>
<td>0.01</td>
<td>-</td>
</tr>
<tr>
<td>Bearing Supply oil pressure Nominal</td>
<td>-</td>
<td>-</td>
<td>0.15</td>
<td>-</td>
</tr>
<tr>
<td>Bearing Clearance Nominal</td>
<td>-</td>
<td>-</td>
<td>0.03</td>
<td>-</td>
</tr>
<tr>
<td>Thermal Interference Prevented</td>
<td>0.9</td>
<td>0.95</td>
<td>0.01</td>
<td>90</td>
</tr>
<tr>
<td>Function or Sub-function Description</td>
<td>Human Action Success Probability Alarm System II</td>
<td>Human Action Success Probability Alarm System I</td>
<td>Frequency of losing goal per year</td>
<td>Consequence of not achieving the goal (lost plant hour operation)</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Bearing Oil Flow Nominal</td>
<td>0.99</td>
<td>0.999</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Oil Viscosity Nominal</td>
<td>0.95</td>
<td>0.985</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Bearing surface Damage and Frictional Heating Prevented</td>
<td>0.974</td>
<td>0.989</td>
<td>-</td>
<td>30</td>
</tr>
<tr>
<td>Failure of Journal Bearing Prevented</td>
<td>0.976</td>
<td>0.989</td>
<td>-</td>
<td>90</td>
</tr>
<tr>
<td>No Foreign Material Allowed to enter Pump</td>
<td>-</td>
<td>-</td>
<td>0.025</td>
<td>-</td>
</tr>
<tr>
<td>Dynamic Loads Within Nominal (Assumed) Limits</td>
<td>0.85</td>
<td>0.92</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Function or Sub-function Description</td>
<td>Human Action Success Probability Alarm System II</td>
<td>Human Action Success Probability Alarm System I</td>
<td>Frequency of losing goal per year</td>
<td>Consequence of not achieving the goal (lost plant hour operation)</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Mechanical Failure of Rotating and Stationary Element Prevented</td>
<td>0.99</td>
<td>0.999</td>
<td>-</td>
<td>250</td>
</tr>
<tr>
<td>Feed Pump Failure Prevented</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>500</td>
</tr>
<tr>
<td>Catastrophic Pump Cavitation Prevented</td>
<td>0.998</td>
<td>0.9992</td>
<td>0.1</td>
<td>-</td>
</tr>
<tr>
<td>Alignment of Stationary And Rotating Elements Prevents Contracts</td>
<td>0.91</td>
<td>0.98</td>
<td>-</td>
<td>150</td>
</tr>
<tr>
<td>Efficiency Degradation of Stationary And Rotating Elements Prevented</td>
<td>0.99</td>
<td>0.9995</td>
<td>-</td>
<td>250</td>
</tr>
</tbody>
</table>
Figure 2: Numerical Evaluation of the Cause-Consequence Nature of Goal Trees Using Decision Trees
Figure 3
Goal Tree For The Feed Pump Example

I. Inlet-outlet
   Enthalpy monitor
II. None

I. CL, Vf
   II. CL

Δ. I. P in the Pump Suction, Vf
   II. P in the pump suction
Figure 3
(continued)

ALIGNMENT OF STATIONARY AND ROTATING ELEMENTS PREVENTS CONTACT

I. (D)
II. None

I. (C, L_s, L_d, T)
II. (C, T)

THERMAL INTERFERENCE PREVENTED

BEARINGS MAINTAIN NOMINAL AXIAL AND RADIAL ALIGNMENT

FAILURE OF JOURNAL BEARING PREVENTED

FAILURE OF THRUST BEARING PREVENTED

BEARING IMPACT DAMAGE PREVENTED

BEARING SURFACE DAMAGE AND FRICTIONAL HEATING DAMAGE PREVENTED

HYDRODYNAMIC PRESSURE OF OIL FILM SUPPORTS LOAD OF SHAFT

BEARING UNIT AREA LOADS IN NOMINAL RANGE

I. (C, oil-p, oil-w, oil-t)
II. (oil-t)

I. (oil-w)
II. None

BEARING OIL FLOW NOMINAL

I. (v)
II. None

BEARING OIL FLOW PRESSURE NOMINAL

OIL VISCOSITY NOMINAL

BEARING CLEARANCE NOMINAL

OIL QUALITY AND CHARACTERISTICS NOMINAL

OIL TEMPERATURE IN NOMINAL RANGE

I. (C)
II. (C)

I. (T)
II. (T)
CL - Clearance (fit), or Alignment monitors
Vf - Vibration frequency monitors
D - Distortion monitor (Due to Thermal Stress)
W - Flow monitor
L_D - Loading - (Dynamic) monitor
L_S - Loading - (Static) monitor
T - Temperature monitor
v - Viscosity measure
P - Pressure
Figure 4: Numerical Evaluation of a Typical Goal Tree Path

Goal Path

Feed Pump Failure Prevented

Mechanical Failure of Stationary and Rotating Elements Prevented

Acute Material Stresses Held Below Ultimate Strength of Material

Acute Stresses Held Below Design Value

Internal Impact Loads Prevented

Catastrophic Pump Cavitation is Prevented

R=0.1(1-0.998)(0.99)(250)

=0.05

R=0

R=0.02

R=0

R=0

R=0

0.1/yr

0.1/yr