Mathematics - Course 121

SOME MODERN RELIABILITY TOPICS

I INTRODUCTION

In this section we will consider such areas as the use of Reliability Data, Failure Mode and Effect Analysis, Fault Trees, Human Factors and Mathematical Modelling, all of which play an important part in the field of Reliability Technology.

II DATA

All Reliability techniques depend for their effectiveness, on good data collection and analysis; the information is used in two forms.

(a) Qualitative: the identification of weak components and the pinpointing of repeated problems is often highlighted only by a formalised data reporting and analysis system. Feedback to design groups and equipment manufacturers is vital for successful design in future plants. It should be realised that many advances in design, militate against high reliability - the call for increased performance, lower cost, less space and weight, less planned maintenance all tend to reduce system reliability. It is therefore important to make design authorities fully aware of the shortcomings of existing plants.

(b) Quantitative: numerical data analysis is useful for:
   i) providing information for accurate prediction of system reliability,
   ii) providing criteria for future plant selection,
   iii) analysing the performance of current systems and identifying unsatisfactory areas,
   iv) demonstrating that current systems meet safety and reliability targets.

The storage of data on component reliabilities is done in two types of databanks.

(a) Generic databanks: large volume banks which have gathered information over many industries, collated this information and presented it in a common format. Data derived from such a bank should be multiplied by a modification factor to suit the environment of the particular application being considered.

(b) Specific plant-based databanks: these are set up within a specific plant, company or industry to provide information on components operating in their own specific environments.

Why use generic data at all? It may be necessary if:

(a) There is no specific plant data available on that piece of equipment

(b) The sample size available in the specific databank is too small to give sufficient confidence in the result

(c) It is necessary to adopt a common database across customers and manufacturers for contract reasons.

III RELIABILITY DESIGN REVIEWS

Generally, Design Reviews are used at stages during the design process, to ensure that the Reliability Programme Plan (RPP) is being followed correctly, and to check on the Reliability activities. If a through-design formal RPP has not been used, then to establish the status of the Reliability work will require a Design Audit. Design Audits are more lengthy and more expensive than Design Reviews.

IV HYDRO SAFETY SYSTEM REVIEWS

These are carried out to ensure that plant systems meet Hydro safety standards and the AECB targets. Two different types of review are carried out.

(a) Safety System Design Reviews: These Reliability analyses are intended to answer the following questions:

(i) Is the overall system reliability acceptable?

(ii) What are the weak points of the system?

(iii) What are the system test requirements?

(b) Operating Reviews: These are done to:

(i) Qualitatively analyse failures experienced during the previous year

(ii) Compare past performance from year to year

(iii) Predict the expected future performance.

V FAILURE MODE EFFECTS AND CRITICALITY ANALYSIS (FMECA)

One of the simplest and most effective tools available to the Reliability engineer is the FMECA. This is a technique which gives the designer a formal method to demonstrate that the effect of component failures within his system has been minimized. It provides an insight into the logic behind component selection and system configuration and is therefore a valuable source of information.

Appendix 1 shows a typical FMECA structure and a simple example. Appendix 2 shows an FMECA which was supplied as part of the handbook for an in-core flux detector amplifier.

After this process has been carried out for the whole system, a grid may be drawn up, rating failure rates on one axis, and severity of effect on the other, see Figure 1. Typically, these are rated on a scale of 1 - 4, but this is a matter of personal choice.

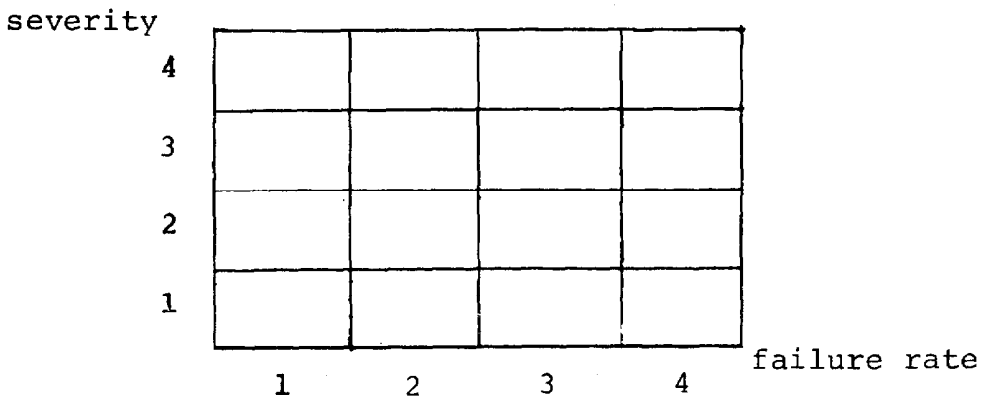


Figure 1: Typical Grid for FMECA

Each line on the FMECA can then be entered in a square on this grid. It is then immediately apparent which failures are most important because of their high failure rates and severe consequences, ie, those falling in the top right hand sections of the grid. This indicates those areas most requiring improvements in reliability.

The best reference on this subject is MIL-STD 1629A - "Procedures for Performing a FMECA" published by the U.S. Department of Defense. This book is a step by step set of instructions for performing a FMECA, and contains sufficient information to allow a novice to construct a successful FMECA.

VI HUMAN FACTORS

Man is the most variable component in any man-machine system; it has been estimated that up to a million independent factors may affect the performance of a single person in any given task, and no one repeats the same task in exactly the same way, however closely controlled are the conditions. It is this variability which makes man so valued by virtue of his adaptability to fit the many roles which society demands. However, this variability also leads to error, and hence to unreliability.

There had been a small amount of work going on during the late 1970's in trying to quantify operator reliability, based generally on the nuclear and chemical process industries. The tempo of this work was greatly increased by the Three Mile Island accident in March 1979, which demonstrated with well publicized effect, how safety and reliability can be reduced by operator error.

Concern for this problem is world wide. In 1979, after three years preparation, the West German Ministry of Research and Technology issued a report which concluded that 72% of all hypothetical core melt accidents would be caused by small reactor pipe breaks. For this kind of accident, about 2/3 of the risk is in human failures and the remainder is in equipment failures. It also concluded that when all kinds of accidents are considered, human error would still be responsible for about 2/3 of the unreliability.

That human failures are the most likely cause of most hypothetical nuclear accidents is also appreciated in the U.S. (see WASH-1400)[1]. In addition, an analysis of the human failure rate in Licensee Event Reports (LER), (filed by the utilities whenever there is some safety-related failure) suggests:

(a) 20-50% of all LER failures are due to human error.

(b) About half the accidents that have led to any release of radiation were caused by human error.

(c) In about 1% of the LER's, there are indications that a safety feature has been severely compromised or made unavailable by human error. For example, at Arkansas No. 1 reactor, loss of auxiliary feedwater occurred on June 17, 1979 as a result of an operator error similar to that which had isolated auxiliary feedwater at Three Mile Island. This was a very pointed case, since it happened just after that plant reopened following a temporary safety check shutdown, ordered as a result of the Three Mile Island accident.

Whilst the use of component failure rate data to calculate system reliabilities is a commonly accepted practice, it might appear impossible to quantify human reliability. However, since the human operator appears to be the most unreliable component in nuclear plant operation, a great deal of effort is being expended, world wide, to do just that.

Appendix 3 shows the results of a small experiment carried out on a gas-cooled reactor simulator. It can be seen that the estimates for operator reliability are far from impressive. One of the largest projects of this kind is under way at Oak Ridge Nuclear Laboratories in the U.S., where a data collection and analysis exercise is being carried out to develop a widely acceptable, comprehensive database for operator reliability.

The most likely outcomes of this type of work are:

(a) The incorporation of the human factor in reactor safety calculations

(b) Increased emphasis on operator training

(c) Regulated requalification of control room personnel

(d) Increased use of simulators in training and operator assessment

(e) Reduced dependence on operator reaction in hazardous situations, hence more automation (already Hydro policy)

(f) Improved control room ergonomics.

VII FAULT TREE ANALYSIS

The Fault Tree is a 'top-down' approach to Reliability prediction, which starts by considering an accident situation. It then considers the possible direct causes of such an accident; next it looks for the origins of these causes. This branching out of causes is what gives the technique the name "Fault Tree Analysis". The approach is the reverse of the FMECA, a 'bottom-up' technique, which starts with individual component failures, and looks for any resulting bad effects. For complex systems, the FMECA becomes a large and detailed document, but it does ensure that every possibility is considered. The Fault Tree is a more compact technique, but its only real output is the final numerical answer, and it is totally dependent upon the imagination of the engineer, to ensure that all significant possible failures and their causes are included.

Each combination of events can be expressed as an AND or an OR statement, and by entering the probabilities of each of the bottom line events, the probability of occurrence of the postulated fault can be calculated.

Example: consider the Fault Tree Analysis of Figure 2 for failure of a car engine to fire.

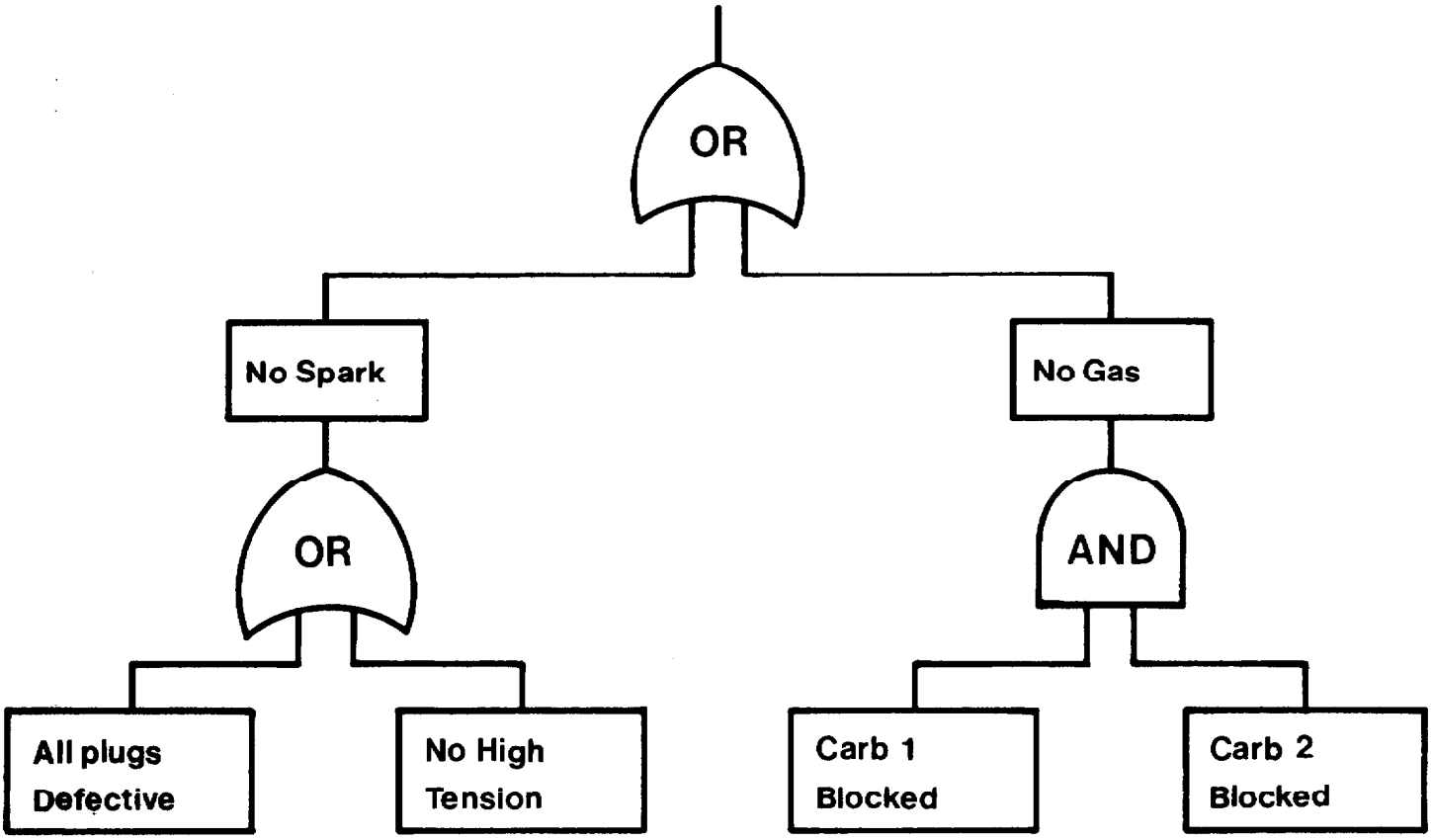


Figure 2: Fault Tree Analysis for Failure of Car Engine to Fire

And if

P(Carb blocked) $= P_C$

P(No H.T.) $= P_H$

P(All plugs defective) $= P_P$

$\therefore$ P(No gas) $= P_C P_C$

P(No spark) $= P_P + P_H - P_P P_H$

P(Engine fails to fire) $= P_C P_C + (P_P + P_H - P_P P_H) - P_C P_C\ (P_P + P_H - P_P P_H)$

Note the shape of the conventional symbols for AND or OR.

This technique is widely used in safety analysis work, since it requires the consideration of only those particular elements which contribute to the top event. In practice, it has the problem of possibly including the same 'bottom event' in more than one limb of the tree; standard computer programs are often used to solve the trees, and these are constructed to knock out the troublesome common elements in the tree. One such program is 'FAUTRAN'.[2]

VIII AVAILABILITY MODELLING

When dealing with large and complex systems, it becomes too difficult to find system reliability using the network methods of lesson 121.00-8. This problem can, however, be treated by a mathematical model which can then be solved by computer. Here we shall look at two types of model.

1. Monte-Carlo Simulation

Monte-Carlo techniques are used if solutions to the problem by analytical techniques or by computation of the probabilistic equations describing the system have proved to be intactible. In the Monte-Carlo process, the system operation is modelled by direct statistical simulation. The name is taken from the random number generator used to predict times to failure.

Simulation of Failure Distributions

Let f(t) be the time to failure probability density distribution for a component. Then

$$Q(t) = \int_o^t f(t^1)\ dt^1$$

represents the probability of the component having failed in time t.

$Q(t)$ is a probability whose value lies in the range (0,1). Accordingly, if one has a table of random numbers in the range (0,1), by choosing one of these numbers, say Q_1, a value of t_1 can be obtained such that

$$Q(t_1) = \int_0^{t_1} f(t)dt = \Theta_1$$

t_1 is then a random value, and is the time to failure predicted from the random number Θ_1.

Four different distributions are in common use:

(a) Exponential: used for simple models

(b) Weibull: preferred for failure rate distributions where component reliability data is extensive.

(c) Normal: used for wearout region.

(d) Log-Normal: preferred for repair rate distributions where data is extensive.

Although Θ_1 is a random number, the shape of the failure rate distribution is governed by the general failure rate data entered into the model. Thus a component with a high failure rate will generally have shorter times to failure than one with a low failure rate.

Model Construction

(a) The system Reliability Block Diagrams are expressed as a series of logic statements, eg, see Figure 3:

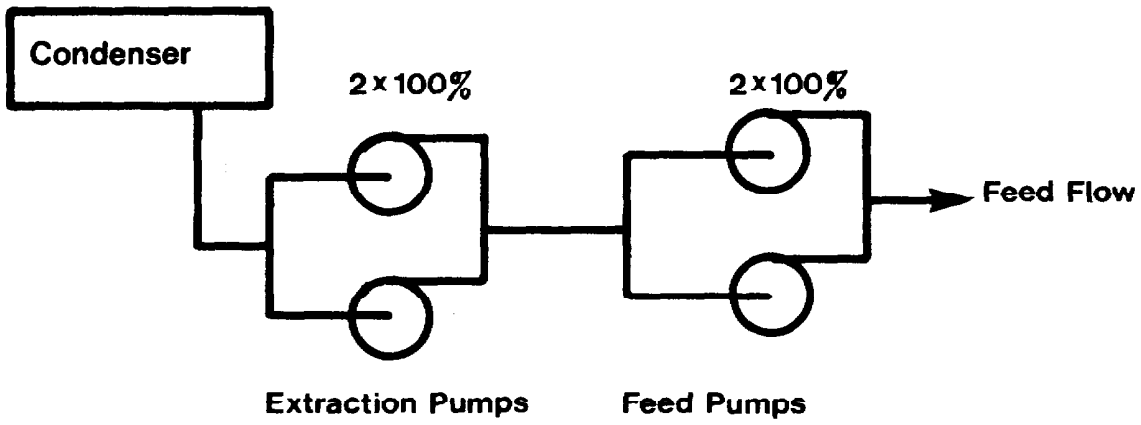


Figure 3: Reliability Block Diagram of a Simple Feedwater System

Feed flow requires condenser AND (extraction pump No. 1 OR
extraction pump No. 2) AND
(feed pump No. 1 OR
feed pump No. 2)

(b) Using the random number generator, a time to fail, and a repair time, are predicted for each component, as demonstrated above.

(c) The mission is run on the computer, with components failing and being repaired at times decided by (b).

(d) At mission end, characteristics such as Availability are computed from the periods of time during which the system was UP, DOWN, DOWN AWAITING SPARES, etc.

(e) The mission is then run again with a different random number seed, and another set of results determined. After a large number of simulations, a statistically significant result can be achieved.

The advantage of Monte-Carlo modelling is its versatility: it is a simple matter to model very many functions, eg,

feed flow for 100% power
feed flow for 50% power
feed flow for 25% power

and such features as standby modes of operation, proportion of repairs possible ON/OFF power, number of repairmen available etc.

The disadvantage of Monte-Carlo modelling is that it requires a very large number of simulations to achieve a reasonable level of confidence in the results. Since the confidence limits are dependent on the number of failures (see Appendix 1, 121.10-1) the technique is not usually suitable for the modelling of highly reliable systems. It is common to run around 2000 simulations just for model testing and proving, and it is often necessary to go to tens, or even hundreds of thousands of simulations to achieve good confidence in the result. This makes it a lengthy process, and one which is expensive in computer running time.

2. Markov Modelling

This is a very different form of modelling which expresses a system's Reliability behaviour in terms of the probabilities of the system being in a particular state, and changing from state to state. This section is designed to show how the Reliability characteristics can be put into a form of mathematics readily handled by a digital computer.

Assume that we have a piece of equipment which can be in one of four mutually exclusive states at any time, these states being:

State 1 - Working normally

State 2 - Broken down and awaiting repair

State 3 - Being repaired

State 4 - Unrepairable

Assume that at any time there is uncertainty as to which state the equipment is in;

Let P_1 be the probability that the equipment is in State 1

Let P_2 be the probability that the equipment is in State 2 etc.

It is convenient to split time up into discrete elements; the time interval being chosen for the convenience of the problem and could be, for example, a minute, an hour, a day or a year. Take for example a time interval of 1 hour.

Then:

P_1 (o) indicates equipment is initially working

P_1 (1) indicates equipment is working after 1 hour

P_1 (n) indicates equipment is working after n hours

The time interval has to be chosen so that the probability of 2 or more transitions, from one state to another, occurring during the interval is negligible.

Let us define α_{ij} as $P(S_i \rightarrow S_j)$, where $P(S_i \rightarrow S_j)$ denotes the probability of a transition from State S_i to State S_j during one time increment.

Then,

α_{11} denotes the probability that the equipment state does not change,

α_{31} denotes the probability that the equipment goes from State 3 to State 1, ie, it goes from being repaired to working normally, etc.

We can now draw up a table of these γ's

To \ From	S_1	S_2	S_3	S_4
S_1	α_{11}	α_{21}	α_{31}	α_{41}
S_2	α_{12}	α_{22}	α_{32}	α_{42}
S_3	α_{13}	α_{23}	α_{33}	α_{43}
S_4	α_{14}	α_{24}	α_{34}	α_{44}

Expressed in a matrix form, this table is called the Transition Matrix T, where

$$T = \begin{bmatrix} \alpha_{11} & \alpha_{21} & \alpha_{31} & \alpha_{41} \\ \alpha_{12} & \alpha_{22} & \alpha_{32} & \alpha_{42} \\ \alpha_{13} & \alpha_{23} & \alpha_{33} & \alpha_{43} \\ \alpha_{14} & \alpha_{24} & \alpha_{34} & \alpha_{44} \end{bmatrix}$$

Since each column denotes all the possible transitions from that particular state, the sum of these probabilities will be 1

ie, $\alpha_{11} + \alpha_{12} + \alpha_{14} = 1$

Let us now describe the probabilities the system being in each of the 4 states at time n by the vector.

$$\underline{P}\ (n) = \begin{bmatrix} P_1(n) \\ P_2(n) \\ P_3(n) \\ P_4(n) \end{bmatrix}$$

where $P_1(n)$ is the probability that the system will be in the 'Working Normally' state at time n. Since each state vector can be obtained by multiplying its predecessor by the transition matrix, we can describe the state of the system at time (n+1) by

$$\underline{P}\ (n+1) = T\ \underline{P}(n)$$

If, at the start of the process, we know that the system is working, we can say that

$$\underline{P}\ (o) = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

and therefore $\underline{P}\ (n) = T^n\ P(o)$

By applying standard techniques of matrix multiplication, the transient behaviour of the equipment can be calculated using a digital computer. This process forms the basis of Markov modelling.

The advantages of Markov modelling are:

(a) It produces a 'point' answer, and does not require the successive simulations of the Monte-Carlo process. It is therefore suitable for modelling even highly reliable systems.

(b) The problem is expressed in a form readily accepted by digital computers.

Markov modelling has the following disadvantages:

(c) It is a complex, mathematically demanding technique which is difficult in conception.

(d) It is much less flexible that the Monte-Carlo method.

(e) The scale of the problem to be tackled is limited by the size of the matrix package available on the computer.

References:

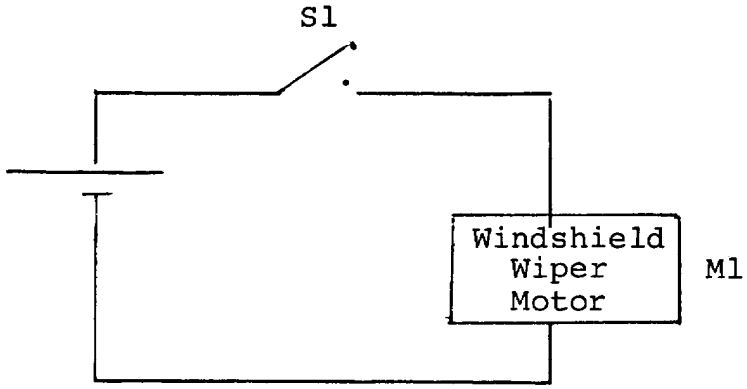
1: Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants (1975) Nureg No. 75-014

2: Wong, P.Y. Fautran - a Fault Tree Analysis Programme. Atomic Energy of Canada Ltd., Ontario.

Typical FMECA Structure

ITEM	DESCRIPTION	FAILURE MODE	FAILURE RATE	EFFECT	SEVERITY (1-4)	COMMENTS
Line 1						
Line 2						
Line 3						

EXAMPLE



ITEM	DESCRIPTION	FAILURE MODE	FAILURE RATE	EFFECT	SEVERITY	COMMENTS
S1	switch	OPEN	$3x10^{-6}$ cycles	wiper won't start	1	--
S1	switch	SHORT	$1x10^{-6}$ cycles	wiper won't stop	2	Consider double-pole switch
M1	etc					

FAILURE MODE AND EFFECTS ANALYSIS

	Description	P.F.R. $f/10^6$ hrs.	Failure Mode	Effects	Seriousness*
J101	Connector, NIM	0.016275	Open contact	No signal or offset at J202. No ± 12V DC.	1
J201	Connector, Lemo	0.110825	Open contact	No response at J202 to input signal but offset still present at J202.	1
J202	Connector, Amphenol	0.219325	Open contact	No signal or offset at P202.	1
C8	Capacitor, tantalum	0.0191	Short circuit	No output at J202. Fuse F1 blown, and no ± 12V DC supply.	1
CR3	Diode, signal	0.010955	Short circuit	Possible loss of all output at J202. Q1 may be shorted base-emitter, ± 12V DC may not be present.	1
CR4	Diode, signal	0.010955	Short circuit	Low amplitude noise spikes may appear at J202. T1 square wave develops spikes at edges of pulses.	2 to 3
CR5-8	Diode, rectifer	0.0056	Short circuit	No signal or offset at J202. No ± 12V DC.	1
R8	Potentiometer wirewound - GAIN	1.4465	Open circuit	(a) Element open between wiper and terminal 1 will cause conversion gain to increase up to 4 times. Offset not effected.	(a) 1

FAILURE MODE AND EFFECTS ANALYSIS

	Description	P.F.R. f/10^6 hrs.	Failure Mode	Effects	Seriousness*
R8	Potentiometer, wire - GAIN	1.4465	Open circuit	(b) Element open between wiper and terminal 3 will cause loss of response to signal at J201. Offset not effected.	(b) 1
R11	Potentiometer, non-wirewound. OFFSET.	1.033	Open circuit	Total loss of offset at J202 or shift in magnitude or polarity.	1
U1	Operational amplifier	5.5	Lead bond breakage	Signal at J202 doesn't respond to signal changes at J201 and output may be noisy.	1
U2	Operational amplifier	0.02238	Lead bond breakage	Signal at J202 doesn't respond to signal changes at J201. Offset at J202 doesn't respond to changes in BIAS control R11 setting. Output may be noisy.	1
U3	Voltage regulator	2.9803125	Lead bond breakage	Varicus depending on location of break but all result in abnormal output voltage from regulator with probable loss of amplifier signal response and offset shift.	1
S1	Switch, pushbutton DET. RESISTANCE TEST	0.27	Open contact	Signal output at J202 will be less for a given input at J201. The lower the resistance of the flux signal detector the greater the reduction in output.	1

FAILURE MODE AND EFFECTS ANALYSIS

Item	Description	P.F.R. $f/10^6$ hrs.	Failure Mode	Effects	Seriousness*
F1	Fuse	0.10	Broken element	Complete loss of signal and off-set at J202. No output from voltage regulator U3.	1

* 1. Amplifier performance severely effected.

2. Amplifier operates with some reduction in performance.

3. Amplifier operates with negligible reduction in performance.

Test characteristic	Fault condition			All faults
	(i) Control rods run out	(ii) Blower failure	(iii) Rise in inlet temp	
Number of tests	9	15	10	34
Estimated time to reach trip level from onset of fault(sec)	64	3	28	--
Operator's Actual response times (sec):-				
minimum	20	1.5	7	--
maximum	64	65	39	--
arithmetic mean	33.6	7.9	19.6	--
Ratio of:- mean of actual operator response times / time to reach trip level	0.53 : 1	2.6 : 1	0.7 : 1	--
Number of failures to trip in time to reach trip level	0	7	2	9
Mean estimated probability of failure	$\frac{0}{9} = 0.00$	$\frac{7}{15} = 0.47$	$\frac{2}{10} = 0.2$	$\frac{9}{34} = 0.26$
Probability of failure of operator to trip plant in time at a 95% confidence level	$\frac{3}{9} = 0.33$	$\frac{12}{15} = 0.8$	$\frac{7}{10} = 0.7$	$\frac{15}{34} = 0.44$

Analysis of Results (Simulator Experiment)

ASSIGNMENT

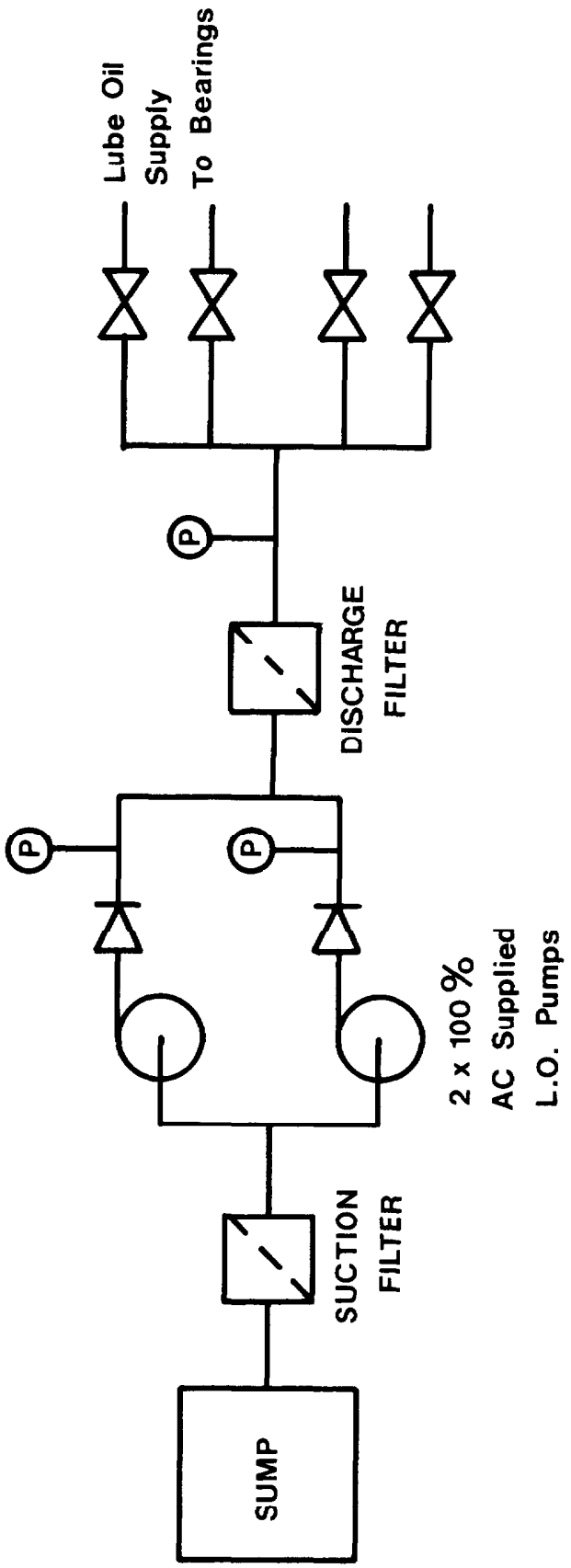
Given a proposed Luboil System as sketched, complete the FMECA table and grid, and make suggestions as to how the reliability of the system could be improved.

Suggested severity criteria:

1. Can be repaired without interruption to oil supply
2. System can be shut down for repair at operator convenience
3. System must be shut down within 10 minutes for repair
4. Total loss of luboil pressure, or requiring immediate system shutdown.

Suggested failure rate criteria:

1. MTTF over 10^5 hours
2. MTTF 10^4 - 10^5 hours
3. MTTF 10^3 - 10^4 hours
4. MTTF less than 10^3 hours.



L.O. Supply System

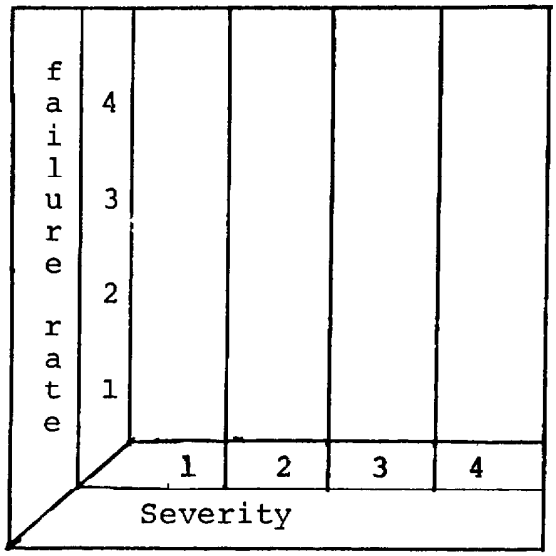
FMECA SHEET 1 of 2

Line Number	Item	Failure Mode	MTTF	Effect of Failure	Severity	Comments
1	Suction Filter	Blocked	$6x10^2$ h			
2	As 1	Air Leakage	$2x10^5$ h			
3	Pump #1 or #2	Shut down	$5x10^3$ h			
4	Electrical Supply to pumps	Total loss	$2x10^4$ h			
5	Discharge NR valve	Open	$8x10^8$ h			
6	As 5	Shut	$6x10^8$ h			
7	Discharge Filter	Heavy Leakage	$5x10^5$ h			
8	As 7	Blocked	$2x10^3$ h			
9	Pump pressure gauge #1 or #2	Loss of Indication	$9x10^3$ h			

FMECA SHEET 2 of 2

Line Number	Item	Failure Mode	MTTF	Effect of Failure	Severity	Comments
10	As 9	Burst	$8x10^4$ h			
11	Pressure gauge -filter dis-charge	Loss of Indication	$9x10^3$ h			
12	As 11	Burst	$8x10^4$ h			

F M E C A GRID



R.B. Malcolm