Review Note

Reliability assessment of mechanical systems

T R Moss, MPhil, CEng, FIMechE, FIQA, FSaRS
Consultant, Abingdon, Oxfordshire

J D Andrews, BSc, PhD, CEng, MIMechE, AFIMA, MSaRS, FSS
Department of Mathematical Sciences, Loughborough University of Technology, Loughborough, Leicestershire

The assessment of mechanical systems is not an exact science and predictions can be subject to considerable uncertainty. In this paper the particular problems of mechanical system reliability assessment are discussed and a general methodology presented based on experience from availability studies carried out on offshore and onshore process plant.

Key words: reliability assessment, mechanical system, safety, availability

1 INTRODUCTION

Reliability and risk assessment techniques are the methods advocated by many regulatory bodies to assess the safety of modern, complex process plant and their protective systems. However, reliability assessment can also be applied to determine the likely availability characteristics of equipment. The trend in manufacturing systems towards large, single-stream plant means that outages due to equipment failures and their subsequent repair can have a significant effect on profitability. Reliability assessment, particularly during the design phase, can be applied to identify the systems, equipment and components that are likely to have a major impact on product availability—this can, of course, include accidents that destroy equipment or part of the plant.

Attention to these reliability-critical areas by the introduction of redundancy and attention to maintainability during the design phase of new plant can lead to dramatic improvements in profitability during the plant lifetime. The methods can also be applied to existing plant, although generally with less dramatic effect since the basic plant design is less easily modified.

Predicting the reliability of mechanical systems does pose special problems. Here these problems are discussed and a basic procedure for carrying our reliability, availability and maintainability assessments is described based on experience from offshore and onshore process plant studies.

2 MECHANICAL RELIABILITY

Models currently employed to predict failure in mechanical process plant are quite elementary. They are largely based on techniques developed many years ago for electronic systems and components. These models can be employed effectively for the evaluation of mechanical systems, but they must be used with caution since they assume that extrinsic factors such as the frequency of random shocks to the system (for example power surges) determine the probability of failure—hence their assumption of Poisson processes and constant hazard rates.

These assumptions are frequently not valid for mechanical equipment. Carter (**1**) shows that intrinsic degradation mechanisms such as fatigue, creep and stress corrosion can have a strong influence on system lifetime and the probability of failure. In highly stressed equipment cumulative damage to specific components will be the most likely cause of failure. Hence a review of the factors that influence degradation mechanisms such as maintenance practice and operating environments becomes a vital element in the evaluation of likely reliability performance. To predict the probability of a high-speed rotating machine failure it will be necessary to identify the various degradation mechanisms and to assess the impact of different maintenance and operating strategies on the expected lifetimes and maintainability of the different components in the system.

The load spectrum generated by different operating and maintenance scenarios can have a significant effect on system failure probability. Carter's research has been published in a number of papers and is summarized in his book, *Mechanical Reliability* (**1**). Essentially his work related failure probability to the effect of the interaction between the system's load and strength distributions (Fig. 1). When these distributions are well separated with small variances (as they are with new equipment in low-stress conditions) the safety margin will be large and the failure distribution will tend towards the constant hazard-rate (random-shock) model. In this case the system failure probability can be computed as a function of the hazard rates for all the components in the system. For highly stressed equipment operating in hostile environments or subjected to fast transients during start-up, the load and strength distributions may have a significant overlap because of the greater variance of the load distribution and the deterioration in component strength with time. Carter shows that the safety margin will then be smaller and the tendency will be towards a weakest-link model. The probability of failure in this case can then depend on the resistance of one specific component (the weakest link) in the system to the applied load excursions.

In between these two extremes the model becomes more complex, incorporating aspects of the random-shock and weakest-link models. An alternative model was proposed by Moss (**2**) in 1987. This model has been further developed at Manchester University (**3**) for the on-line prediction of failure probability for a wet-gas compressor. In this development a reliability assessment of the compressor system was first performed using the

The MS was received on 22 April 1995 and was accepted for publication on 28 February 1996.

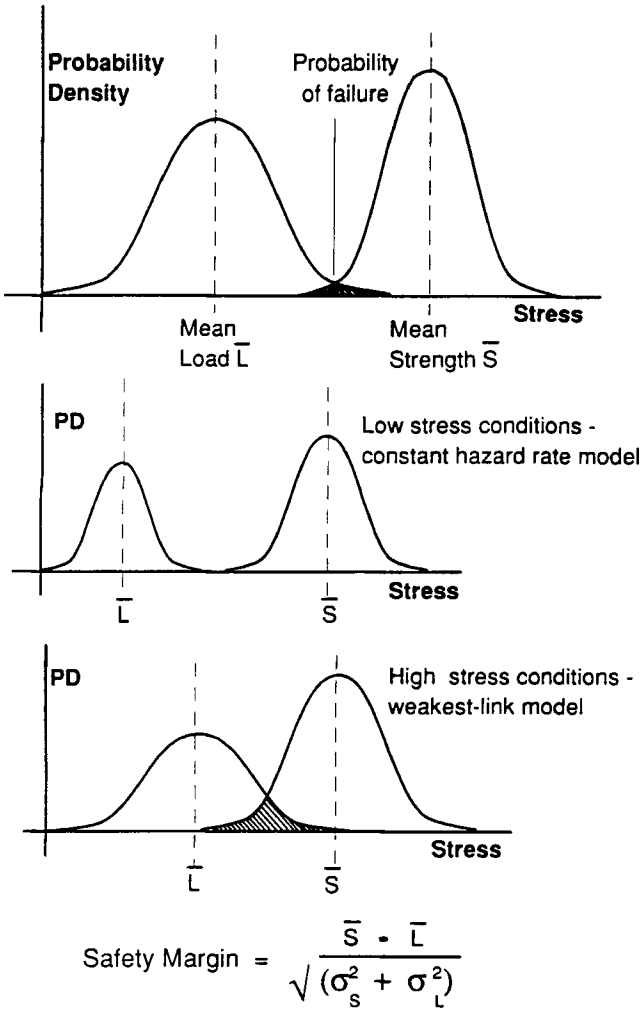

Fig. 1 Interaction of load and strength distributions

constant hazard-rate model and the system failure probability predicted using generic reliability data. Changes in the monitored load-parameter distributions (which are assumed to reflect component strength changes) were then input to the model to continuously update the prediction of the system residual lifetime.

Catuneanu and Milhalache (**4**) have also considered mechanical system reliability and have proposed a Markov chain model for systems subject to age-dependent failures which may recover to the initial state or to a degraded state. They propose the use of fault tree analysis to identify the minimum cut sets leading to failure and simulation to determine the lifetime distribution as a function of age. The component reliabilities are related to the real stresses by an approach similar to that of Carter. These models of mechanical reliability are interesting from a theoretical point of view but no detailed examples or actual applications are given in the text.

Bloch and Geitner (**5**) describe more practical methods for assessing machine reliability based on the age of the equipment, the environment and the duty cycle. The procedures are well defined and examples, with comprehensive check-lists to be applied in association with failure mode and effect analysis, are given for a wide range of equipment. In the United Kingdom similar methods have been applied with some success for the prediction of safety-critical failures in large reciprocating pumps by Lewis and Carrick (**6**). Martin (**7**) and Hughes (**8**) have both proposed methods for modelling dependent failures, the former adapting Carter's approach to predict potential failures for a gearbox and the latter considering the effect of different environments (including the maintenance environment) on the probability of simultaneous failure in redundancy systems.

In all of the foregoing studies, however, the lack of comprehensive data on equipment failures and load distributions can be identified as the main limitation of these models for mechanical system reliability assessment. Thus for large mechanical plant an approach based on the assumption of constant hazard and repair rates in conjunction with sensitivity analysis appears to be the best currently available to identify the reliability-critical items. Subsequently, checks on the effect of operating and maintenance policy can then be carried out during the design review stage to evaluate their likely impact on degradation processes, failure frequencies and repair/replacement times.

3 RELIABILITY PREDICTION

3.1 General

With mechanical systems and particularly those containing rotating machinery, the prediction of reliability performance is not straightforward. There can be considerable variance in the failure frequencies and average repair times of components which are not revealed by conventional methods of reliability analysis. Although the basic reliability analysis techniques such as failure mode and effect analysis and fault trees can be applied in mechanical system assessments, there is a need to consider and limit the effects of component degradation. Operational, environmental and maintenance conditions which may affect the validity of the generic reliability/maintainability data used in assessing equipment and system availability also need to be studied. A subjective evaluation of the factors which can lead to uncertainties in the basic data is necessary to ensure that predictions based on the assumption of constant hazard rates are sound. Design decisions can then be taken with a reasonable degree of confidence.

Reliability is generally defined as the probability that a system, equipment or component will operate successfully for a stated period of time under stated operating and environmental conditions. In this definition reliability is employed as a generic term covering unrepairable and repairable systems. For plant where the systems are repairable, the repair process as well as the failure process needs consideration. It is usual (because of the relative limitations of the failure/repair data available) to consider steady state operation when the plant is assumed to have settled down and thus failure time and repair time are random variables. For this steady state model the availability, A, the probability to function on demand, is also a random variable and is defined as the ratio of the uptime to the total time. Hence

$$A = \frac{\text{MTTF}}{\text{MTTF} + \text{MTTR}}$$

where

MTTF = mean time to failure

MTTR = mean time to repair

With this simple expression it is possible to calculate global estimates of the availabilities of equipments and to combine these logically to determine the expected availability of a system.

This expression is satisfactory when the plant can only operate in two states: up (working) or down (not working). Where the plant can operate at different levels of output the availabilities in the different operational states must be determined. The output availability of the plant is then the sum of each operating state availability multiplied by the product output level for that state. For a plant with n up (output) states and one down state the product availability would be:

$$\text{Product availability} = \sum_{i=1}^{n} (\text{availability } i \times \text{level } i \text{ output})$$

For example, if an offshore production platform can exist in either one of two output states producing 100 000 or 50 000 barrels of oil per day with availabilities of 78 and 18 per cent respectively (and downtime unavailability of 4 per cent), then the average output availability of the platform is

$$A(\text{output}) = \frac{0.78 \times 100\,000 + 0.18 \times 50\,000}{100\,000} = 87\%$$

(that is an average production rate of 87 000 barrels of oil per day).

4 PROCEDURE FOR ASSESSMENT

For the reliability assessment of complex systems a consistent, logical approach is essential. The plant specification, engineering drawings, process diagrams and other documentation alone can make a paper mountain several feet high, so that isolating the basic information needed to carry out the assessment can present quite a problem. For most process plant an effective approach can usually be made by concentrating on the piping and instrumentation diagrams (PIDs). Using these drawings with the plant specification and process flow diagrams as the initial information base the assessment can proceed along the following lines:

1. Review the information available and write down a brief description of the process.
2. Define:
   (a) assessment objectives,
   (b) plant and system boundaries,
   (c) inputs and outputs across boundaries,
   (d) plant operational states,
   (e) failure criteria,
   (f) assumption made in the availability model.
3. Develop a simplified functional block diagram for the installation and logic diagrams such as fault trees for each output state down to a system/subsystem level (the indenture level) at which relevant failure and repair data can be obtained.
4. From the fault trees and output-state information, develop an availability model for the installation and check generic sources of failure, repair and production data for input to the model.
5. Assemble a set of PIDs for the systems, draw in subsystem boundaries and evaluate subsystem availabilities. Where relevant data are not available use failure mode and effect analysis or parts count techniques.
6. Review these data against the operating states and failure criteria, adjust for the plant operational/environmental conditions and insert into the availability model equations. Estimate the availabilities of the systems and plant and compute the average output availability of the installation.
7. Rank the systems and subsystems by their availability scores.
8. Carry out a sensitivity analysis for the low-availability items to determine the effect of changes in the input data on the predictions. Where the changes are significant review the data sources and recalculate the availabilities with the modified data.
9. Consider the effects of degradation mechanisms induced by design, operation and maintenance procedures/environments on component lifetimes, system failure frequencies and repair times at the design review stage. Recommend QA (quality assurance) procedures (including condition monitoring) or design modifications to control their effects.
10. Write a report highlighting the reliability-critical areas with recommendations on design, maintenance and operation relevant to availability performance.

The methods are described in more detail elsewhere, for example by Andrews and Moss (**9**, **10**) and Davidson and Hunsley (**11**). Here the application of the two main techniques—failure mode and effect analysis (FMEA) and fault tree analysis (FTA)—employed in mechanical system reliability studies are discussed with examples from actual assessments.

5 ASSESSMENT TECHNIQUES

5.1 FMEA

Failure mode and effect analysis is a powerful reliability assessment technique developed by the American defence industry in the 1960s to address the problems experienced with complex electronic, weapon-control systems. Subsequently it was extended for use with other electronic, electrical and mechanical equipment. It is a step-by-step procedure for the systematic evaluation of the failure effects and criticality of potential failure modes in an equipment design. FMEA can be applied at different indenture levels, for example to determine the availability characteristics of a gas compressor operating on an offshore oil production platform or the failure-on-demand probability of its fire protection system, down to an evaluation of the failure mechanisms associated with a pressure switch. By the analysis of individual component failure modes, the effect of each failure on system operation can be determined.

FMEAs can be performed in a variety of different ways depending on the objective of the assessment, the stage of equipment development and the information

400 KW CHILLER UNIT

INDENTURE LEVEL -2
Sheet no. 6 of 20
Mission Phase 1 - OPERATING

Study by:
Prepared by:
Approved by:
Date:

SYSTEM Ref-Description-Function	FAILURE		POSSIBLE CAUSES	SYMPTOM DETECTED BY	EFFECT OF FAILURE		Compensating provision against failure	REMARKS
	Entry code	Mode			Local	On next level		
1.4.0 Lubrication system Provide cooled lube oil at pressure to bearings and gearing. Auxilliary oil pump from starting, Jet pump and low and high speed centrifugal pumps whilst running. Duplicate filters and single lube oil cooler.	1401	Leakage	Loose connectors. Auxiliary oil pump fault.	Observation - gas in air monitors. Fall of sump level.	Slow leaks have no effect.	Eventual shutdown if uncorrected by loss of oil pressure. Performance loss if air ingress.	2-hourly inspections. Automatic shutdown on low oil pressure.	Sump contains 30 litres, so a loss of say 25% acceptable to unit, should be readily observed.
	1402	Oil too hot	Restriction of oil flow. Restriction of water cooling. Fouling of heat exchanger.	High oil temperature warning.	Inadequate lubrication due to low oil viscosity and loss of bearing cooling.	Eventual shutdown.	Unit shutdown due to high lube oil temperature.	Slow rise of oil temperature would be found by study of readings.
	1403	Oil pressure low	Blockage. Wear. Jet pump faults.	Low oil pressure warning.	Inadequate lubrication due to reduction of oil flow.	Eventual shutdown.	Unit shutdown due to low lube oil pressure.	Oil pressure is one of the most important parameters monitored. Will be watched to decide on state of oil filter.
	1404	Oil contaminated	Filter not cleaning oil. Water in oil.	Daily observation of oil condition.	Discolouration and/or emulsification of oil.	Eventual damage if not corrected.	Oil condition is judged daily. Oil is changed annually.	Condition of "replaced" oil filters is examined for evidence of an abnormal state.
	1405	Oil level in sump low	System leak. Oil transfer to refrigerant circuit.	Observed in sight glass.	Only sudden severe leak would have effect.	Sudden, severe leak would lead to shutdown on low lube oil pressure.	Pre-start-up checks and daily checks. Sudden severe leak gives shutdown or low oil pressure.	Oil can be topped up, a standard routine. When sufficient oil has migrated to refrigerant it can be returned slowly.
	1406	Oil level in sump high	Refrigerant in oil.	Observed in sight glass. Foaming.	Reduced lubrication due to gas separating out from oil.	Eventually no output. Shutdown or low lube oil pressure.	Pre-start-up checks and daily checks. Pre-start requirement to keep oil hot for 12 hours.	Gas separating out from oil would give low lubricating oil pressure shutdown.

Fig. 2 Functional FMEA worksheet

available on its components at the time of the analysis. The objective of the FMEA must be clear—whether to identify, say, weak areas in the design, the safety-critical components or perhaps maintainability-critical items. The FMEA focus may dictate a different worksheet format in each case; nevertheless, there are two basic approaches:

1. The functional FMEA, which recognizes that each item is designed to perform a number of functions which can be classified as outputs. These outputs are identified and loss of essential inputs to the item or internal failures are then evaluated with respect to their effects on system operation.
2. The hardware FMEA, which sequentially lists individual equipment items and analyses the effect of each item failure mode on the operation of the system.

In many cases a combination of these two approaches is employed. For example, a functional analysis at plant and major system levels, followed by more detailed analysis of the hardware shown to be sensitive to the range of uncertainties in the failure data is employed in the initial functional, 'broad-brush' analysis.

The FMEA worksheet is tabular in format to foster a systematic approach to the analysis. A standard worksheet layout is shown in Fig. 2. The column headings generally employed are:

Item identity/description: a unique identification code and description of each item
Function: a brief description of the function performed by the item
Failure mode: each item failure mode is listed separately—there may be several for an item
Possible causes: the likely causes of each postulated failure mode
Failure detection method: features of the design through which the failure is recognized
Failure effect—local level: the effect of the failure on the item's function
Failure effect—system level: the effect of the item failure mode on system operation
Compensating provisions: any internal compensating provisions which could mitigate the effect of the failure
Remarks: comments on the failure mode/effect including any recommendation for action

If the analysis is extended to quantify the severity and probability of failure (or failure rate) of the system (defined as a failure mode and effect criticality analysis—FMECA) further columns may be added to the worksheet, such as:

Severity: the level of severity of the effect ascribed to each failure mode classified as:
- Level 1—minor, no effect on item functional performance
- Level 2—major, degradation of item functional performance
- Level 3—critical, severe reduction of item functional performance resulting in a change in the system operational state
- Level 4—catastrophic, complete loss of system function

Loss frequency: the expected frequency of loss resulting from each failure mode, either as a failure rate or failure probability. The latter is usually estimated for the operating time interval as a proportion of the overall system failure rate or failure probability (F). The levels generally employed for process plant are:
- (a) Very low probability $<0.01F$
- (b) Low probability $0.01–0.1F$
- (c) Medium probability $0.1–0.2F$
- (d) High probability $>0.2F$

Part failure rate λ_p: the overall failure rate of the equipment or part in its operational mode and environment. Where appropriate, application and environmental factors may be applied to the generic data to adjust for the difference between the conditions associated with the generic failure rate data and the operating stresses under which the item is going to be used.
Failure mode proportion α: the fraction of the overall failure rate related to the failure mode under consideration
Probability of failure effect β: the conditional probability that the failure effect occurs.
Operational failure rate λ_0: the product of λ_p, α and β
Data source: the source of the failure rate (or failure probability) data

A one-sheet example from an FMECA is shown in Fig. 3.

For FMECAs a criticality matrix similar to the one shown in Fig. 4 is constructed relating loss frequency to severity for each failure mode. Failure mode identification numbers are entered in the appropriate cell of the matrix according to their loss frequency and severity. The critical item failure modes which may require further study are shown in the top, right-hand cells.

FMEA worksheets are frequently developed for very specific applications, for example to provide input to an RCM (reliability centred maintenance) analysis or a plant availability study. One sheet of a simplified functional FMEA for the availability assessment of the separator module of an offshore plant is shown in Fig. 5. Here consideration of the failure modes has been restricted to the proportion that can cause a forced outage of the system. Average repair times are included and combined with the aggregated failure rate to estimate the availability of this subsystem.

5.2 Fault tree analysis

There are two approaches that can be used to analyse the causal relationships between component failures and system failure. These are inductive or forward analysis and deductive or backward analysis. FMEA is an example of inductive analysis. As seen from the previous section, it starts with a set of component failure conditions and proceeds forward, identifying the possible consequences; this is a 'what happens if' approach. Fault tree analysis is a deductive 'what can cause this' approach and is used to identify the causal relationships leading to a specific system failure mode—the 'top event'.

The fault tree is developed from this top, unwanted event, in branches showing the different event paths.

LUBRICATION SYSTEM
REF. DRAWING – XY2123
OPERATIONAL STATE – Normal operation

Date:
Sheet 8 of 20
Originator:
Approved:

IDENTITY/ DESCRIPTION	FUNCTION	FAILURE MODE	FAILURE EFFECT		FAILURE DETECTION METHOD	COMPENSATING PROVISIONS	SEVERITY	LOSS FREQUENCY ($F/h \times 10^6$)				DATA SOURCE	REMARKS
			LOCAL	SYSTEM				λ_p	α	β	λ_0		
22.2 Oil heater	Maintain lube oil temperature	22.2/1 Heater unit failure	Violent foaming of oil during start-up	Low lube oil temperature - fluctuating oil pressure	Oil temperature gauge	Pre start-up checks include oil temperature readings	2	73	0.4	1.0	29	HARIS Reliability Data Handbook	Heat maintains lube oil temperature during SD
		22.2/2 External leak	Loss of lube oil from system	Bearing or seal failure on drive unit	Visual level gauge on oil reservoir	Bearing temperature high alarm. Automatic drive unit S/D on HH alarm	2	73	0.6	0.3	13		
22.3 Lube oil reservoir													

Fig. 3 Hardware FMECA example

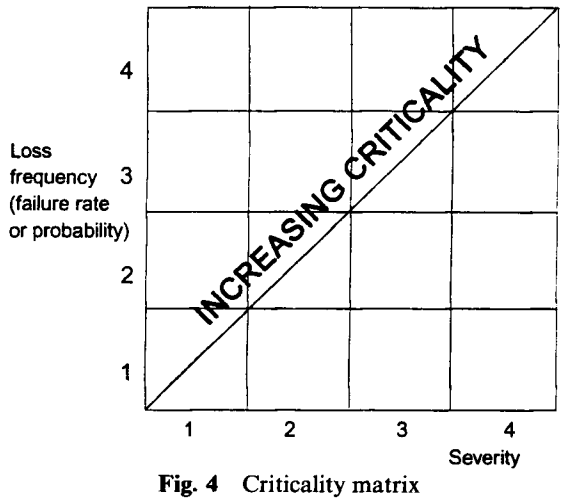

Fig. 4 Criticality matrix

Component failure events represented in the tree are progressively redefined in terms of lower-resolution events until the basic events on which good-quality failure data are available are encountered. The events are combined logically by use of gate symbols as shown in Fig. 6, which shows the structure of a fault tree. In this case the basic event combinations that could result in total loss of output from a simple cooling water system are developed. Using this failure logic diagram the probability of the top event or the top event frequency can then be calculated by providing information on the basic event probabilities.

The top event and the system boundary must be chosen with care so that the analysis is not too broad or too narrow to produce the results required. The specification of the system boundary is particularly important to the success of the analysis. Many systems have external power supplies and other services such as a water supply. It would not be practical to trace all possible causes of failure of these services back through the distribution and generation systems; nor would this extra detail provide any useful information concerning the system being assessed. The location of the external boundary will be partially decided by the aspect of system performance that is of interest; however, it is also important to define the external boundary in the time domain. For example, the start-up or shut-down conditions of a plant can generate different hazards from its steady state operation and it may be necessary to account for this in tracing the fault.

Within the assessment procedure described previously the detailed steps required to perform a fault tree analysis can be summarized as:

1. Identification of system failure states for analysis
2. System understanding
3. Logic model generation
4. Qualitative evaluation of the logic model
5. Data analysis
6. Quantitative evaluation of the logic model
7. Uncertainty analysis
8. Sensitivity/importance analysis

Many of these steps are the same whatever system is being analysed, though there are some aspects which mean that special attention must be devoted to the different stages when mechanical systems are involved.

Having performed steps 1 to 4 and carried out a qualitative evaluation of the fault tree, the minimal cut sets (combinations of component failures which provide the necessary and sufficient conditions for system failure) are produced.

To progress further with the analysis requires the component failure probabilities, $q(t)$, to be determined. Typical models utilized in commercial fault tree evaluation codes would be as follows:

$$q(t) = \frac{\lambda}{\lambda + \nu}(1 - e^{-(\lambda+\nu)t}) \tag{1}$$

for revealed failures where λ is the component failure rate and ν the repair rate and

$$q_{AV} = \lambda\left(\tau + \frac{\theta}{2}\right) \tag{2}$$

for unrevealed failures, where q_{AV} is the average unavailability, τ is the mean time to repair and θ is the test interval. For safety systems that are normally inactive, failures are only revealed during test, which means that the unrevealed failure model is appropriate for these systems. However, the underlying assumption in both of these models is that the failure and repair rates are constant, giving a negative exponential distribution for the probability of failure (repair) prior to any time t.

Constant failure rates are associated with random failure events as indicated by the useful life period of the 'bathtub curve'. Mechanical components subject to wear, corrosion, fatigue, etc., may in many cases not conform to this assumption. If the quality of data available permits a statistical distribution to be fitted to the failure times then other distributions such as the Weibull may provide a more accurate description of the data. This is also true for the repair times which can commonly be described by normal or log-normal distributions.

When either the failure or repair rates are not constant and probability density functions for the times to failure $f(t)$ and repair $g(t)$ are available, then they can be combined to give the unconditional failure intensity $w(t)$ and unconditional repair intensity $v(t)$ by solving the following simultaneous integral equations [see reference (9)]:

$$\begin{aligned} w(t) &= f(t) + \int_0^t f(t-u)v(u)\,du \\ v(t) &= \int_0^t g(t-u)w(u)\,du \end{aligned} \tag{3}$$

Having solved these the component unavailability is then given by

$$q(t) = \int_0^t [w(u) - v(u)]\,du \tag{4}$$

For the case of constant failure rates $f(t) = \lambda_e^{-\lambda t}$ and $g(t) = \nu_e^{-\nu t}$, equations (3) can be solved by Laplace transforms. Substituting the solution obtained into equation (4) yields equation (1). For more complex distributions of failure and repair times, numerical solutions may be required.

PLATFORM - GEORDIE ALPHA
SUB-SYSTEM - 1ST STAGE SEPARATOR

SYSTEM - OIL PROCESS
DRAWING(S) - P & ID 005

Sheet 1 of 4

IDENTITY	DESCRIPTION	FAILURE MODE	FAILURE EFFECTS	FORCED OUTAGE FAIL RATE (F/YR)	RESTORATION TIME (HRS)	DOWN TIME (HRS/YR)
V210A	Separator vessel	Internal mechanical failure	Liquid level out of control, level alarms initiate ESD, inlet valve XEA2 closes. Process shut-down.	0.12	24	2.88
XEA2	ESD valve (12" ball valve, pneumatic actuator)	a) Valve stuck open	a) No effect while running. Alarm on shutdown. Restart inhibited.			
		b) Valve stuck shut	b) Start up inhibited (25%)	0.26	8	1.56
		c) Actuator failure	c) Valve closes (fail-safe). Process shutdown (50%).			
LEA4	Pressure transmitter	Fails to 'Alarm' state	ESD valve XEA2 closes Process shutdown.	0.35	2	0.7
FCV3	Oil flow control valve (6" globe valve, pneumatic actuator)	a) Valve stuck open	a) No effect, but LEA11 will initiate process shutdown if no action taken.	0.26	8	2.08

Fig. 5 First-stage separator FMEA for availability estimating

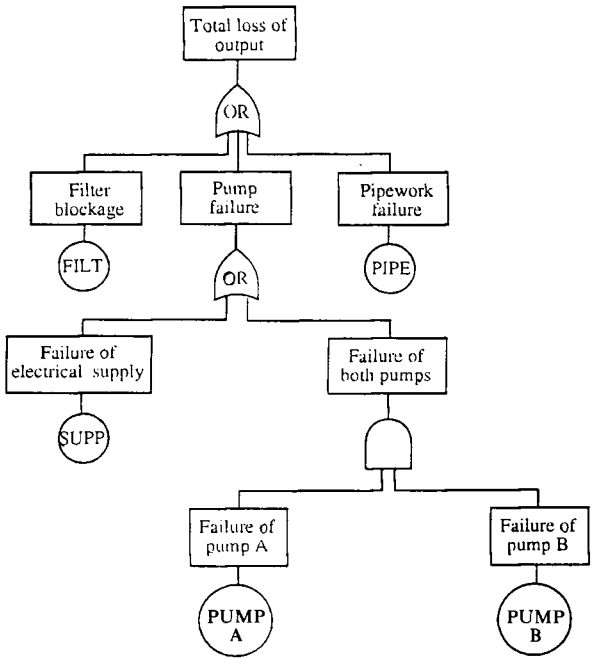

Fig. 6 Fault tree example

With the components data produced at step 5 the fault tree quantification can produce:

(a) the system failure probability,
(b) the system failure rate and
(c) the expected number of system failures.

Where failure and repair distributions have been specified for the analysis, confidence intervals can be determined at step 7. Step 8 produces the importance rankings for the basic event which identifies the components that provide the most significant contribution to system failure.

Fault trees are, of course, significantly more complex for real engineering systems than that illustrated in Fig. 6. Figure 7 shows part of a fault tree developed to represent the failure of a ventilation recirculation control system in an under-sea mine. For this analysis it was required that ventilation recirculation was stopped in certain 'unsafe' conditions such as when carbon monoxide or methane was detected in the mine. Certain components in this study were shown to have failure times that were represented by the Weibull distribution and an accurate analysis would therefore require the solution of equations (3).

The main use of fault trees is in safety and risk studies. Fault trees provide a useful representation of the different failure paths which can lead to unavailability of systems and plant even without considering failure and repair data—which may provide some difficulties. In many cases, therefore, fault trees and failure mode and effect analysis will be employed in combination—the FMEA to define the consequences of specific equipment failures and the fault tree (or possibly several fault trees) to identify and quantify the paths that lead to plant unavailability.

6 SIMULATION

An alternative approach to system assessment, which requires no simplifying assumptions to be made regarding independence of failure and repair events or the form of the distributions, is simulation. It is a computer intensive approach which is now becoming more popular due to the continuous advances being made in computer technology. This has resulted in the processing power required for simulation to be available at relatively modest prices.

The simulation technique, due to its generic nature, can offer some useful features appropriate to mechanical systems. The first is the ability to model any form of distribution for failure and repair times. As outlined above, it is possible to accommodate this requirement within the fault tree analysis technique. However, as far as the authors are aware, none of the available commercial codes features this capability.

Maintenance activity has a very important influence on the reliability of mechanical systems. Simulation can model scheduled maintenance outages, maintenance activity prioritization and queuing of repair jobs. Over the coming years it is highly likely that this technique will provide the most appropriate means of analysis for mechanical systems.

7 FACTORS AFFECTING MECHANICAL SYSTEM ASSESSMENTS

The steps in the reliability assessment of a plant or system are summarized in Section 4. More details of these steps are given in references (**9**) and (**11**), which also provide example case studies of their application in availability assessments. As noted in these case studies and reiterated in this paper, a major cause of uncertainty in the prediction of mechanical system availability is data. Failure rate data for large, complex items of mechanical plant are a particular problem because of uncertainties concerning the boundaries and the operating/environmental conditions of the items from which the generic failure rates were derived. Mean outage times (repair and waiting times), which are necessary to predict item availability, can also pose problems since they depend on the equipment design and the variety of conditions peculiar to each plant. These include the operations and maintenance policy, availability of spares, access for maintenance and many other factors.

Maintainability analysis is essential for mechanical system assessments and unfortunately is an area largely ignored by reliability specialists. Some useful research has been carried out in one or two limited areas, for example the subjective analysis by Thompson (**12**) of pipe couplings. The *OREDA (Offshore Reliability Data) Handbook* (**13**) includes estimates of repair times in addition to failure rates for quite a wide range of mechanical equipment, and since this is a very specific functional environment associated with clear definitions of system boundaries the data may be employed in global assessments with some degree of confidence.

The basic requirement is for assurance that the different factors that can affect the reliability performance of an equipment in a specified environment have been considered and their effect on generic failure and repair rates evaluated. The objective should be to identify the degradation mechanisms that could apply in each case and then to assess the tolerance of the system to such mechanisms and the compensating provisions in the

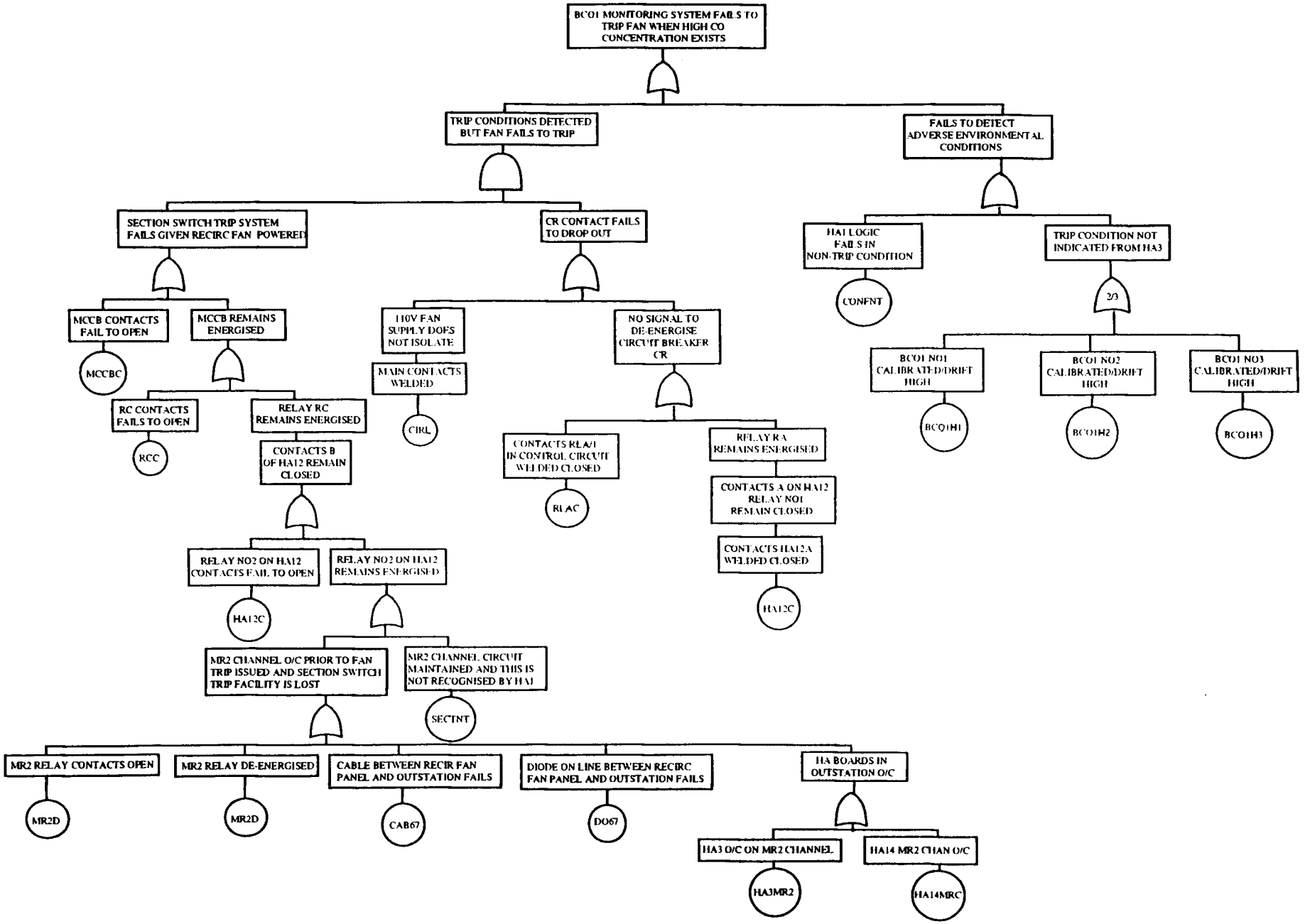

Fig. 7 Fault tree for the unrevealed failure of system 1

AMMONIA PLANT

DISTRIBUTION OF EQUIPMENT DOWN TIMES (HOURS/YEAR)

UNIT		Rotating Machinery			Valves				Heat Exchangers	Boiler Units	Est'd Hours Lost	Est'd Days Lost	% of Total Est'd Lost Days
		Turbines	Compressors	Other	Pneumatic	Hand	PRV	MRV					
03	Steam Boilers									175.2	175.2	7.3	15.5%
13	Syngas Compressor	84	43		4.2	1.8	1.2		2.9		137.1	5.7	12.1%
08	Raw-Syngas Compressors	42	60		5.1	3.3	0.6	0.4	3.6		115.0	4.8	10.2%
12	N_2 Compressor	42	38	29		0.6	4.0	2.0	2.9		118.5	4.9	10.4%
15	Refrigeration	42	38		12.0	2.1	12.0		12.5		118.6	4.9	10.4%
09	Rectisol			3.5	19.9	11.5	4.8	8.0	40.0		87.7	3.7	7.9%
14	NH_3 Synthesis				12.6	1.8	0.2		58.3		72.9	3.0	6.5%
02	Air Compressors	21	22.5	23	2.8	1.7	1.0		1.5		73.5	3.1	6.6%
01	Air Separation			2.7	32.2	7.7	3.6	3.6	2.1		51.9	2.2	4.7%
10	CO Conversion				0.9	2.8	2.0	4.0	36.0		45.7	1.9	4.1%
Estimated Hours Lost		231	201.5	58.2	89.7	33.3	29.4	18.0	159.8	175.2	820.9h		
Estimated Days Lost		9.6	8.4	2.4	3.7	1.4	1.2	0.8	6.7	7.3	41.5d		
% of Total Estimated Lost Days		20.4%	17.9%	5.1%	7.9%	3.0%	2.6%	1.7%	14.3%	15.5%			88.4%
		43.4%			15.2%				14.3%	15.5%			
		88.4%											

Fig. 8 Analysis of predicted plant outages

design that could mitigate their effects. For example, the principal degradation mechanisms likely to influence reliability performance of a large, continuously operated gas turbine driving a high-speed centrifugal hydrocarbon gas compressor in an offshore environment are fatigue and wear. Attention to oil analysis and vibration monitoring during operation should ensure that appropriate maintenance action is taken before a major failure can develop. With this provision the random-shock (constant hazard-rate) model could be appropriate.

Reliability performance could be significantly different for a similar gas turbine driven HC gas compressor operated intermittently in the onshore environment of a gas-distribution network. The failure rates, failure modes and repair characteristics are likely to be quite different in these two environments, requiring a totally different approach to maintenance and testing. In this case high stresses can be generated due to acceleration and temperature transients during start-up. A weakest-link model may then be more appropriate since degradation will be less easily detected.

The operating regime, environmental conditions and maintenance strategy are the factors that need particular attention in mechanical system availability assessments. Failure mode and effect analysis in association with fault trees and a subjective analysis of equipment maintainability should ensure that the potential high outage time failure modes associated with material degradation are identified at the design stage. Appropriate condition monitoring systems should be specified to ensure that these potentially high outage time failures are revealed before the system deteriorates significantly. Maintenance actions can then be planned for the next time the plant requires a shut-down. If degradation-type failures are anticipated and eliminated before they develop, the constant hazard-rate reliability model will be appropriate for mechanical systems. Random shocks to the system cannot be anticipated so predicted availabilities at that stage will be the best that can be achieved without introducing additional redundancy or other design changes. However, the failure tolerance of alternative systems can in some cases be significantly higher and some loss of process efficiency may be a worthwhile price to pay for a system with a higher availability potential.

An example of one output from a major plant availability study is shown in Fig. 8. The distribution of outage times for this 1000 tonne/day ammonia plant is arranged as a matrix showing the predicted downtime of the top 10 systems (out of 23) and the contribution by the main equipment classes. It is notable that the predictions were generally confirmed during the first year of operation. Such a matrix clearly shows the areas that will need particular attention by maintenance engineers during the plant lifetime.

8 CONCLUSIONS

The availability of mechanical equipment can have a significant impact on plant profitability; hence availability assessment of new installations should be an essential part of the design process.

Standard methods for equipment reliability assessment, such as failure mode and effect analysis and fault trees, can be effective if precautions are taken to ensure that likely degradation mechanisms are identified and measures introduced (such as condition monitoring) to minimize their contribution to plant downtime. Alternative techniques such as Monte Carlo simulation may become more popular for this aspect over the next few years.

The operating and maintenance regimes can have a very significant influence on mechanical plant availability. Unless precautions are taken to anticipate the onset of mechanical equipment degradation major failures associated with long outage times are likely to occur from time to time. Where degradation effects cannot be monitored and controlled the constant hazard rate model is not an adequate representation of likely reliability performance.

REFERENCES

1 **Carter, A. D. S.** *Mechanical reliability*, 2nd edition, 1986 (Macmillan).
2 **Moss, T. R.** On-line acquisition and analysis of mechanical failure data. IFIP Conference, Dubrovnick, 1987.
3 **Harris, M. J.** and **Mann, R. S.** Development of a microcomputer-based system 'SHARP' for on-line monitoring of the reliability characteristics of rotating machinery. Third ESReDA Seminar on *Plant ageing and maintenance*, Chamonix, 1992.
4 **Catuneanu, V. M.** and **Mihalache, A. N.** *Reliability fundamentals*, 1989 (Elsevier).
5 **Bloch, H. P.** and **Geitner, F. K.** *An introduction to machinery reliability assessment*, 1990 (Van Nostrand Reinhold).
6 **Lewis, J.** and **Carrick, H.** Machinery safety registration and verification of critical machines. IMechE Seminar on *Maximising rotating machinery reliability*, 1994.
7 **Martin, P.** A systematic approach to interactive failures. Seminar on *Mechanical reliability*, Tribology International/NCSR, 1980.
8 **Hughes, R. P.** A new approach to common-cause failure. *Reliability Engng*, 1987.
9 **Andrews, J. D.** and **Moss, T. R.** *Reliability and risk assessment*, 1993 (Longman).
10 **Andrews, J. D.** Quantitative safety assessment of the ventilation recirculation system in an undersea mine. *Qual. and Reliability Engng*, 1991, 7(6).
11 **Davidson, J.** and **Hunsley, C.** *The reliability of mechanical systems*, 2nd edition, 1994 (Mechanical Engineering Publications, London).
12 **Thompson, G.** The comparative design evaluation of pipe joints with respect to reliability. IMechE Seminar on *Valve and pipeline reliability*, 1993.
13 OREDA. *Offshore reliability data handbook*, 2nd edition, 1992 (DNV Technica).