Trans IMarE, Vol 102, pp 191–199

Failure mode and effect analysis of a subsea production system

***F J Deegan, BEng and †D J Burns, MSc, CEng**
*R M Consultants Ltd and †W S Atkins Engineering Sciences Ltd

SYNOPSIS

This paper deals with a design technique called Failure Mode and Effect Analysis as applied to a remote subsea production system located in the North Sea. Many marginal offshore oil fields are now developed having used subsea production systems. Due to the nature of such systems it is important that such systems are cost effective and reliable. One method of achieving such a design aim is to use the technique called Failure Mode and Effect Analysis (FMEA). The purpose of an FMEA, in general terms, is to detect potential areas of design weakness in order to allow time for the design to be changed or operating procedures to be amended. The technique of FMEA postulates failure modes of components and follows them through the system to an 'end effect', using a set format worksheet. This FMEA was performed to DNV Guidelines 1–85 'Safety and Reliability of Subsea Production Systems'.

The paper describes in detail the FMEA technique and the system analysed. This includes the method by which problem areas were highlighted to the design team. This allows actions to be raised and implemented before the design is frozen. Finally the technique allowed the reliability critical areas to be highlighted for inclusion in the operating manuals. The discussion includes the safety features inherent in the design which mitigate certain failure modes.

INTRODUCTION

Marginal offshore oil fields are now developed using subsea production systems. This is now a recognised production technique, but certain design criteria have to be applied to ensure cost effective and reliable solutions are obtained. In order to achieve some of these aims Failure Modes and Effect Analysis (FMEA) have been applied to the development of a field in the Norwegian sector of the North Sea. The basis of the analysis is to identify a particular CAUSE or FAULT MODE within the system and trace forward the logical sequence of this condition through the system to the final effect. That is the technique is a CAUSE – EFFECT type.

Francis J Deegan is a Senior Consultant with R M Consultants Ltd in Warrington. He has worked in safety and reliability for 6 years, and his project experience covers the defence, nuclear, aerospace, chemical and offshore industries. He has worked for several consultancies in the UK and is a specialist in offshore safety and reliability. Mr Deegan has a Batchelor of Engineering degree from the University of Bradford.

David J Burns is a Principal Engineer in the Safety and Reliability Department of W S Atkins Engineering Sciences Ltd in Epsom. His experience covers 22 years in the nuclear, chemical and offshore industries engaged in system safety, reliability and development. The major part of his career has been spent with ASEA (now ABB) in Sweden. He has an MSc in Chemical Engineering from UMIST and is a Chartered Engineer.

PURPOSE OF AN FMEA

The purpose of an FMEA is, in general terms, to detect potential weaknesses or 'reliability critical areas' and to identify their sensitivity in order that design, operational and/or maintenance modifications can be made to improve reliability.

While the objective of an FMEA is to identify all modes of failure within a system design, its first purpose is the early identification of all catastrophic and critical failure possibilities so they can be eliminated or minimised through design correction at the earliest possible time.

Although basically it is concerned with 'modes of failure' and 'effects of failure' much more information can be obtained, dependent on the reasons for the FMEA. The use of the FMEA is called for in maintainability, safety analysis, logistics support analysis, maintenance plan analysis, and for failure detection and isolation at subsystem level. In looking at the 'effects of failure' these effects may also be considered at local level or at subsystem or even overall system level.

As part of the FMEA process each potential failure can then be evaluated in terms of its expected frequency of occurrence (failure rate) and the severity of the failure effect. Finally, the integrated hazard frequency can then also be determined (this being the sum of the product of the frequency of failures resulting in like consequences).

TIMELINESS IN THE USE OF THE FMEA

The usefulness of the FMEA as a design tool and in the decision making process is dependent upon the effectiveness with which design weaknesses are communicated for early design attention. Probably the greatest criticism of the FMEA has been its limited use in improving designs. The chief causes for this have been untimeliness and/or the isolated performance of the FMEA without adequate inputs to the design process. Timeliness is perhaps the most important factor in

Component name	Ref	Function	Op mode	Failure mode	Failure cause	Local effect	End effect	Detection method	Compensating provision	Severity	Remarks
Valve block	2.0.1	To allow gas condensate to flow through a series of remotely controlled or ROV operated valves as required by the needs of the production facility.	NP WW WK	Leakage of gas condensate from the master valve block.	Leakage due to seal failure or structural failure of the master valve block body or loss of locking of the actuators or flowlines.	Leakage of gas condensate from the hydraulic actuator to master valve block body seals, or from the flowline, control or instrument outlet seals to the external environment. Structural failure of the master valve block body causing leakage.	Leakage of the gas condensate from any of the actuator, instrument, or flowline attachment points. Minor leakage will result in slight loss of production and some pollution. Severe leakage or structural failure will result in the complete loss of production and severe environmental pollution.	Possible environmental pollution. Reduced production flow rate. A gas detection system is included. Loss of pressure within the system.	The surface controlled subsurface safety valve can be operated to shut down production and facilitate the repair/replacement of the X-mas tree during the next workover operation. The master valve body block should be tested to API procedures for subsurface cracks prior to assembly.	4A 2B 2C	
		To retain pressure within the flowline between the tubing hanger and the master valve block outlets.	NP WW	Failure of the master valve block assembly to retain pressure within the system.	Failure of the production stab seals (2.0.18) to retain production pressure.	Leakage of gas condensate from the main production flowline to the annulus around the master valve block bottom flange.	Failure to retain the system pressure within the flowline will result in a build up of pressure in the master valve block bottom flange. Possible leakage of gas condensate into the external environment should the AX gaskets fail.	Loss of pressure within the system will be detected by the pressure monitor on the main flowline.	The production stab seals have one metal to metal seal and two elastomer seals. The sealing of the stab seals is tested when the X-mas tree is installed on the wellhead. To have the original failure result in any pollution would require a second failure of the pressure retaining system.	4A 2B 2C	Severity dependent upon extent of the leakage.

Fig 1: Typical failure mode and effect analysis worksheet

differentiating between effective and ineffective implementation of the FMEA.

Therefore, as a rule, the FMEA should be initiated as soon as the preliminary design information is available at the higher system levels, and extended to the lower levels as more information becomes available on the items in question. An important point to note though is that on very large systems the amount of information produced by a detailed FMEA can be too large to handle. Therefore care must be exercised in the use of the FMEA technique.

Statoil as part of the design of subsea production systems require that DNV Guidelines 1–85 'Safety and Reliability of Subsea Production Systems',[1] are complied with. These guidelines are aimed at providing assurance that there is adequate safety built into the design to guard against:

1. loss of life;
2. significant environmental pollution;
3. major economic loss.

As part of the verification that the subsea production system satisfies these requirements a failure effect analysis should be carried out. This failure effect analysis is to deal with the most probable failures, their probability and consequences. Such failure types may be technical, operational or due to accidental loading. The results of this analysis should govern the design of the system, and the content of the operation, in-service inspection and testing manuals.

The guidelines, in addition to these failure effect requirements, provide various points to note when carrying out the failure effect analysis, some examples being:

1. Yielding of the protective structure due to accidental loads of small probability might be acceptable when supported by the failure effect analysis.
2. The feasibility of disconnection and re-entry of the riser strings, with due respect to safety for the subsea production system and the riser itself, should be considered in the failure effect analysis.

The guidelines, if complied with, will enable a Statement of Compliance for a subsea production system to be issued by Veritas.

DNV FAILURE MODE AND EFFECT ANALYSIS

The aim of this particular analysis is to ensure compliance with the guidelines with respect to effects of failures on safety and detectability. The guidelines state as a minimum that a 'detailed FMEA should encompass the subsurface safety valve and the wellhead and hanger system. Control and Monitoring Systems of these safety systems should also be included'. Similar analyses should also be made for other systems of special importance, eg 'riser systems'.

The FMEA should include all failure modes, eg technical failures, failures due to accidental loading and operational failures. In particular attempts should be made to identify failure modes which reduce or destroy the safety functions of the equipment and in particular:

1. failures from a common origin, eg failures that are caused by the events that make use of the safety barrier necessary;
2. a failure mode introduced during normal operation and testing;
3. failure modes occurring when the system is in the activated mode;
4. detection possibilities of individual failures;
5. effects of the failures on safety.

With this as the basis for the study the DNV 1–85 format shown in Fig 1 was used for compliance with the DNV 1–85 guidelines.

Perhaps the most important aspect in any FMEA is an accurate and consistent definition of severity levels. It is most important that these definitions are agreed in detail prior to the start of the study or extensive reworking of the analysis will be required. With this as the basis the DNV guidelines primary aim in using the failure effect analysis is to highlight failure events which could cause Very Critical Events (VCEs) and Critical Events (CEs) to occur.

The guidelines define a VCE as a failure which results in:

1. loss of control of the well;
2. and/or loss of life.

CEs are defined as a failure which results in:

1. one well barrier remaining or two barriers remaining with the working status of one barrier unknown;
2. damage to subsea equipment resulting in damage to several wells or at least one well and manifold damaged;
3. evacuation of personnel necessary.

As these definitions were not directly applicable to the system being analysed it was necessary to rework them. Therefore, after a certain amount of discussion with the operator, designer and the analyst, the reworking resulted in the subdivision of each severity ranking into three categories as follows:

A. personnel safety;
B. production delay;
C. environmental pollution.

The results of this subdivision enabled emphasis to be placed on which failures are contributing to a particular risk picture for personnel safety, production delay or environmental pollution (see Fig 1).

Level 1 (VCE – very critical event)

1. possibility of death or severe injury to personnel;
2. loss of production resulting in more than 3 months lost production and/or loss of control of the well;
3. extensive environmental pollution.

Level 2 (CE – critical event)

1. severe direct injury to personnel;
2. damage to the facility resulting in a loss of production of between 7 days and 3 months and/or one safety barrier remains, status known, or two safety barriers remain but status of one unknown.
3. severe environmental pollution – major threat to the environment.

Level 3

1. minor injury to personnel;
2. damage to the facility resulting in less than 7 days lost production;
3. minor threat to the environment.

Level 4

1. no direct injury to personnel;
2. slight or no damage to the facility;
3. no threat to the environment.

Critical events, summary

Once an event has been identified as either a VCE or a CE it is a requirement to summarise these on separate worksheets.

Component name	Ref	Failure mode	End effects	Detection	Action	Prob	Comment
4 1/6" (manual) lower master valve (LMV).	2.0.2	The valve fails to close when operated by an ROV.	The gas condensate continues to flow through the X-mas tree. Reduced redundancy.	The valve position indicator on the ROV panel. The pressure and temperature probe readings from the production bore of the X-mas tree.	Tubing recoverable surface controlled subsurface safety valve (TRSCSSV) can be closed in a well shut down sequence. Test the operation of the lower master valve at regular intervals.	II	Further additional facilities are provided within the X-mas tree to allow the flow of gas condensate to be stopped. This valve will only be used as a final backup system. The valve should be tested at regular intervals to check for correct operation.
4 1/16" production swab valve (PSV).	2.0.4	Spurious closure of the valve during a well kill.	Unable to equalise the pressures in the bores or to complete the killing of the well. Possible blowout from the well.	Loss of the hydraulic signal can be detected at the workover rig control panel.	If a diver/ROV is present then the valve can be opened manually.	III	The valve is designed to fail safe in the event of loss of hydraulic pressure.
Riser coupling.	4.1	External leak.	Leakage of wellbore fluids(during workover). Possibility of pollution. Cannot pressure test tree etc, after installation.	Extensive leaks will be apparent from pressure drop or resulting pollution.	Retrieve and rerun tree if pressure test fails.	I	Pressure test each join before it is employed. Both annulus and bore joint have two independent elastomeric seals.
Standard riser joint (and pup joint).	4.2	Structural failure (cracking) due to overload, fatigue or design or manufacturing errors.	Leakage of fluid during workover. Possibility of pollution. Cannot pressure test tree etc. Crack may lead to massive structural failure.	Pressure drop.	Use of spare riser joints or repair.	I	Pressure test joint before deployment.

Fig 2: Very critical events listing

These lists then provide an input into the operations manuals which will be held on the platform. A typical example of such a listing is shown in Fig 2. This gives a description to the 'operator' on how the failure mode can be detected in the control room and possible actions which can be taken to mitigate the failure.

This ranking system and the calculation of probability of failure for VCEs enables the analyst to concentrate design attention on the most serious events. A VCE may be identified but from failure data the probability of occurrence may not warrant design changes due to the very low probability of occurrence. On the other hand though extensive design changes may be required. These would hopefully be at the design stage so saving extensive time and effort later on.

Failure rate data

For the reliability information both field data and engineering judgement were used. The main source of field data was the OREDA handbook,[2] although certain failure rates were obtained from other sources which are available in-house and relevant to the offshore industry. Examples of the data used are shown in Table I.

The FMEA analysis in addition to calculating severity and probability levels will raise other areas of concern. Therefore throughout the analysis, in order to record such points, a system of Corrective Action Reporting Forms (CARFs) was raised by the analyst. An example of such a form is shown in Fig 3. The CARFs were raised for both the FMEA and for discrepancies between the equipment design and the equipment specification. For each CARF raised, the comments of the equipment designers were noted and the FMEA revised where appropriate. The CARF forms provided a very useful method of monitoring the progress of actions raised within the design process. They also provide evidence to the user of the system that an independent check on points, other than failure modes, was considered by the FMEA analyst.

Table I: Examples of failure rate data

Component	Failure rate per 10^6h
Tree block failure	1.0×10^{-7}
Tree cap	2.0×10^{-9}
Gate valves	1.0×10^{-6}
AX gaskets	2.0×10^{-6}
Flowline connector	2.0×10^{-6}

FIELD DEVELOPMENT DESCRIPTION

The field is a gas condensate field and comprises two separate structures with hydrocarbon accumulation from the Cretaceous age. The two structures have been named Alpha (South) and Gamma (North).

The field will be developed with a subsea production system on both the Alpha and Gamma structures. A remote platform of an existing field will be used as a control and receiving point. Each structure will be developed using a template comprising six wellheads on each.

Part A: Definition of need for corrective action	Part B: Project management response
1. REFERENCE (SPEC) Part of the specification requires a seal test facility on the Christmas tree. It is not evident how this test can be accomplished. It is recommented that such a test is incorporated in the design.	√ ACCEPTED – (ACTION PLAN DESCRIBED BELOW) MODIFIED – (ACTION PLAN DESCRIBED BELOW) REJECTED – (FOR REASONS GIVEN BELOW) Plan/Explanation: A test port is shown on the machine detailed drawing for testing this seal. Part C: Corrective action implemented Description: None MOD NO PREPARED BY: DATE: APPROVED BY: DATE:
2. PREPARED BY: DATE: 3. APPROVED BY: DATE: 4. RESPONSIBLE ORGANISATION(S) 5. CARF FORWARDED TO: DATE:	Part D: Completion of Corrective Action I confirm that the FMEA follow through is complete TEAM LEADER SAFETY: DATE:

Fig 3: Corrective action form

Considering the economic potential a subsea production system was the most cost effective solution for exploiting the field. Although the complete subsea production system would require a FMEA analysis this paper only covers part of the equipment used.

Equipment

The equipment which was analysed for the Subsea Development Project using FMEA was basically the wellhead and workover system. The overall system breakdown was as outlined below:

1. tubing hanger system;
2. christmas tree;
3. lower riser package;
4. completion workover riser;
5. surface flow tree.

From reference to system design specifications and understandings gained from discussion with the design engineers etc, a system block diagram was drawn up. This system block diagram is shown in Fig 4.

Subsystem breakdown

Due to the size of these systems it was necessary both to break the systems down into more manageable blocks and to agree upon the modes of operation which each component was to encounter.

As an example of this the following subsystems were identified within the major system of the christmas tree.

Christmas tree system

1. valve block and associated valves;
2. christmas tree mandrel;
3. tree connector;
4. flow loops;
5. flow loop connectors;
6. hydraulic multiplex system;
7. christmas tree cap;
8. christmas tree running tool;
9. production guide base and mountings;
10. tree cap running tool.

From the above system breakdown a further more detailed functional block diagram was drawn up. For the christmas tree system this is shown in Fig 5. The purpose of these functional diagrams was to aid in the functional description of the operation of the systems, these diagrams then provided the basis for the analysis. They also indicated the fact that in order to analyse the system a relatively detailed FMEA was required. Therefore, now, at this stage, the point to be considered was the method by which this FMEA was to be performed.

There are two general approaches to FMEAs namely; the hardware approach and the functional approach. The hardware approach is normally utilised in a part level-up fashion (bottom up approach), while the functional approach is normally utilised at a higher indenture level-down fashion (top down approach). From the size of the system to be analysed and the convenient blocks into which it had been broken it was decided to use the functional approach. In addition, as noted earlier, the hardware approach would have produced too many worksheets for further meaningful analysis.

OPERATIONAL CONSIDERATIONS

Further points which required consideration in the FMEA of a subsea production system concerned such factors as installation methods, maintenance regimes, and well safety barriers. Without due consideration of each of these factors the FMEA would have appeared incomplete. In order to examine their bearing on the FMEA each of these factors is considered in further detail below.

Installation

The equipment will, with the other wellhead equipment, be installed on the production template using a semisubmersible drilling rig. In this installation phase diving support will be required for connecting flowloops etc. It is expected though that during the life of the system, which is expected to be 20 years, various other interventions using a drilling rig will be required.

Maintenance (interventions)

A major consideration in any subsea production system is the methods used to maintain the system, and its frequency. The nature of the design means that preventative maintenance has to be planned well in advance. Such factors which have to be considered are repair vessel availability and the number of possible working days available within each month. Obviously factors such as these affect production availability. In addition to these the type of repair required influences the workover scenario required.

There are two types of workover used, namely 'Wireline' and 'Major'. Major workovers will be used on this system for such operations as christmas tree change-out of downhole safety valve replacement. These will utilise a semisubmersible or jackup rig and should in principle be diverless, and based on remotely operated vehicle (ROV) assistance for such operations as overriding christmas tree valves.

Wireline workover will be used for such maintenance activities as replacement of the christmas tree control pod. Wireline workover will make use of a diving support vessel or other small support vessel.

Therefore for an effective FMEA to be carried out the frequency of preventative maintenance activity has to be known. The assumptions made in this study were:

1. that one wireline workover lasting up to 2 weeks each year on each wellhead would be performed;
2. that one major workover lasting 2 weeks every 5 years would be carried out.

Corrective maintenance would be carried out to repair certain failure modes postulated in the FMEA. Therefore throughout the FMEA consideration was given to the workover regimes required, and possible methods on the workover highlighted.

Finally, in any workover scenario, it is important to remember that the time required to perform an intervention is dependent upon the type of intervention required. This is influenced by the arrangements made for support vessels etc. In addition, the type of repair required for each failure mode has to be known by the analyst, as the time factor for repair is considered in the severity rating of the system. The assumptions made with regards to these points were as outlined below:

1. unscheduled major workovers required to carry out maintenance take longer than 7 days to initiate;
2. an intervention requiring only a diver/ROV requires between half a day and 7 days to initiate.

Well safety barriers

Finally, the analysis did not cover such safety barriers as the downhole safety valves or the choke/kill valves situated in the blow out preventer (BOP). The possibility of using such valves to mitigate the end effects of failure was noted on the FMEA sheets. In accordance with DNV 1–85 failures of any safety systems having an effect that also results in the requirement to use a safety system were treated as VCEs. In this study the safety systems of interest were:

1. the SCSSV control lines;
2. wireline cutter valves;
3. valves on the christmas tree.

Operational modes

From this information and knowledge of the system, therefore, the following modes of operation were agreed upon:

1. normal production mode (NP);
2. wireline workover (WW);
3. major workover (MW);
4. well kill (WK);
5. installation and test (I/T);

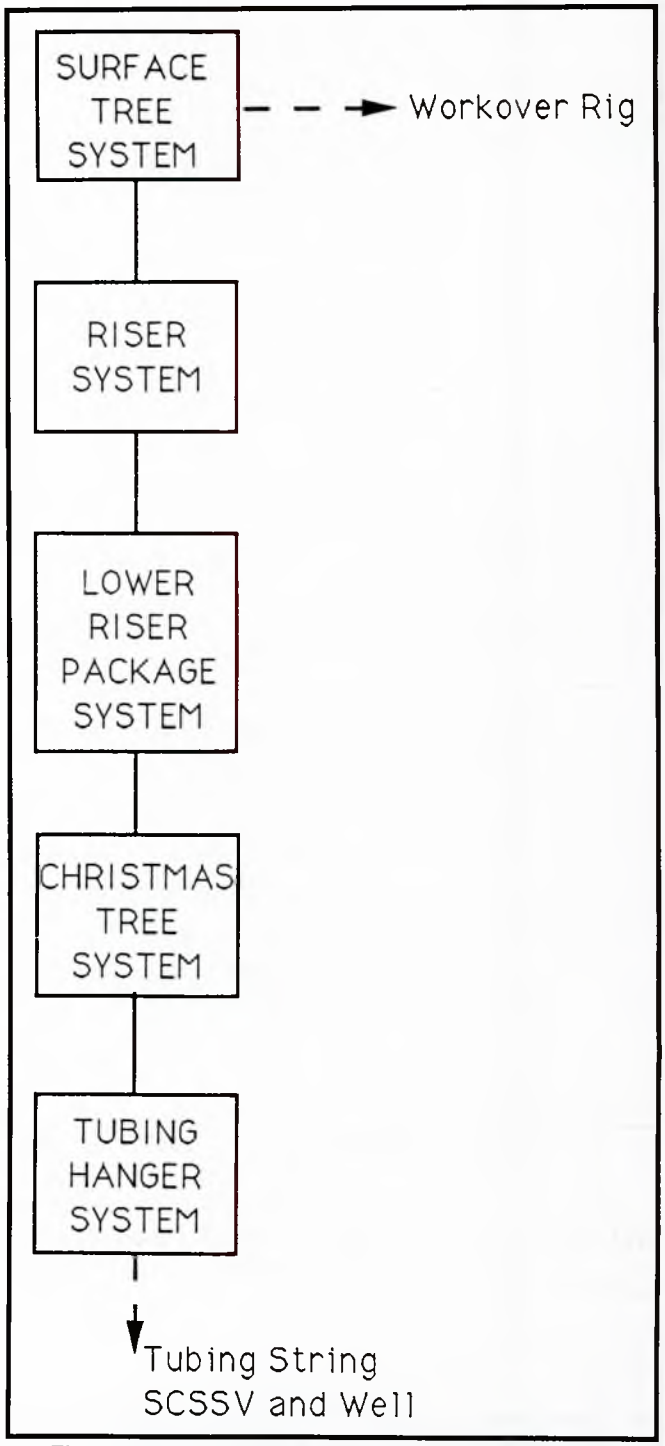

Fig 4: Workover functional system block diagram

Table II: Surface flow tree operational modes

System component	*Operational mode* NP	WW	MW	WK	I/T
4 1/16" Production master valve	X	X			T
4 1/16" Production swab valve	X	X			T
2 1/16" Annulus swab valve	X	X			T
4 1/16" Production wing valve	X	X			T
2 1/16" Annulus wing valve	X	X			T

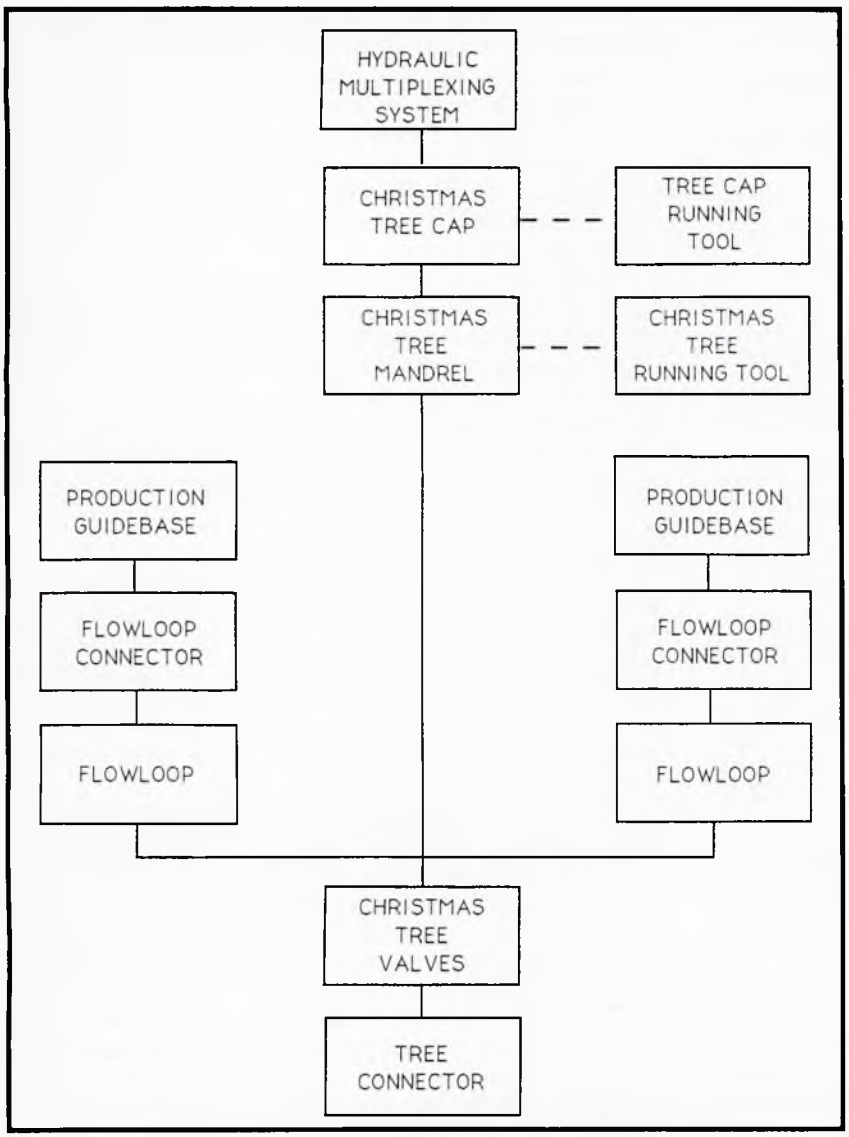

Fig 5: Christmas tree functional block diagram

Table III: Breakdown of failure modes for each system, outlined on 77 worksheets

System	*No of sheets*
1 Tubing hanger system	11
2 Christmas tree system	44
3 Lower riser package system	8
4 Completion and workover riser system	7
5 Surface flow tree system	7

In order to ensure that all the failure modes, operating modes etc, were covered, a matrix was drawn up which cross referenced subsystems with operating mode. A small section of the matrix (surface flow-tree) is shown in Table II.

THE FMEA

Now that the scene has been set the FMEA can be carried out. To illustrate the FMEA the christmas tree system is considered in some detail here. The christmas trees function can be described as an 'interface device which can isolate and control the flow of crude oil as it leaves the ground and starts its way along a flowline to the place of collection.' The christmas tree is generally a collection of valves, actuators, seals, pipes and associated controls, as well as a means of connecting the flowline to the wellhead. On a subsea production system the christmas tree has to allow the low riser package (LRP) to be inserted when workovers are to be undertaken. This LRP then allows risers to be attached so that direct communication can be made with the surface tree on the workover rig.

In the FMEA analysis detailed consideration is given to the valves and sealing mechanisms, as these are the primary functions. Some detailed functional failure modes considered were:

1. the valve is stuck open and refuses to close when commanded;
2. the valve is stuck closed and refuses to open when commanded;
3. the valve will operate but not to the full extent of its travel;
4. the valve gate and/or its sealing faces have become damaged and the valve will not seal;
5. leakage occurs from the christmas tree block or one of the sealing faces.

Failures of the valves will result in reduced or total loss of control of the well fluid. Leakage from the tree block will result in lost production and environmental pollution entailing a requirement for a major workover.

As the sealing of the wellhead and christmas tree is a major area of concern, special emphasis was placed on this function during the FMEA. Seal failure can result in leakage of well or control line fluids within the systems and result in erosion/damage to the sealing face. This, if not repaired, could result in extensive damage occurring over a period of time. Therefore, throughout the FMEA, whenever a seal leak was identified checks were made for back up seals. The use of redundant back up seals is one method by which the inconvenience of leaking seals is overcome. The most common method used in this design for the provision of back up sealing systems was the use of two elastomeric seals combined with a back up metal to metal gasket. Quantification of such sealing system failures cannot be carried out in an FMEA as this method only covers single failures. The most appropriate method for quantification is fault tree analysis. The means by which the FMEA identified such back up provision is by noting them under the 'Compensating provisions' column of the worksheet.

As the FMEA will be used to provide an input into the operating procedures manuals it is important to note the method by which failures can be detected. From review of the equipment specification three methods were generally used to detect failures. The first of these methods was by use of the various instruments mounted on the christmas tree. These were used for pressure and temperature measurement. They enable the control equipment located on the platform to monitor both well fluid status and completion annulus pressure. The second method was to carry out extensive tests whenever a system was installed prior to actual use. The third method used concerned

the valves on the tree. For remote valve position indication the monitoring of the flow of hydraulic fluid from the reservoir, whenever a valve was operated, was used. Therefore throughout the FMEA the method of detecting a failure was noted in the appropriate column of the worksheet. These are later extracted for the VCEs and included in the operating manuals.

RESULTS OF THE FMEA

This was a very detailed FMEA study which covered many aspects of the design and resulted in a total of 257 different failure modes for different parts of the system. These failure modes were outlined on 77 worksheets which were broken down for each system as shown in Table III.

Of the 257 different failure modes only 4 were defined as VCEs and 65 as CEs. Additionally each failure mode had at least one method by which it could be detected. If detected it would allow the operators to take appropriate action to avert any further damage. For the majority of failure modes at least one compensating provision has been included in the design in order to mitigate the initial failure. Finally, the CARF system provides a method of noting design weaknesses to the designers at an early stage. Some of the points raised concerned areas of sealing systems, where discrepancies between the design and design specification were noted. All of the CARFs issued were replied to and resulted in no outstanding areas of design weakness.

The general result of the analysis is that the design of the system conformed to the requirements of DNV Guideline 1–85 in that at least two independent failures would have to occur before a safety system is affected.

Summary of very critical events

The VCEs are all identified as critical single point failures within separate subsystems. Two of the VCEs concern failure of the valves in the christmas tree and two failures in the riser system. All would result in pollution of the environment and lost production provided they are coincident with other safety system failures. The coincident failures required were generally outside the scope of the FMEA. To illustrate the nature of the VCEs, they are described in narrative form below. Included in the narrative is the coincident failure of the safety system required to result in loss of well control, leading to the postulated end effect.

1. Failure of the manual lower master valve (LMV) to close is regarded as a failure of a safety barrier. The LMV would only be closed if the downhole safety barrier has failed and there was a possibility of leakage from the tree itself. To result in total loss of control the hydraulic upper master valve would also have had to fail to close. Therefore the LMV will only be used as a back up to the remaining valves on the christmas tree. As a precaution against failure of this valve it was recommended that it should be tested for operational readiness at regular intervals.
2. Spurious closure of the production swab valve (PSV) during a well kill is a failure which could lead to a possible blowout situation due to the inability to equalise pressures in the completion system. The standard precautions taken before any workover is carried out should prevent the development of such a situation.
3. The two VCEs identified for the riser system are single point failures which will result in pollution of the environment. The extent of the pollution is dependent upon the extent of the failure. If the correct operating procedures are undertaken the possibility of such a failure occurring will be very much reduced. If the failure should occur it is possible for it to be detected and for the safety barriers to be operated, thereby preventing extensive pollution.

To conclude the christmas tree system has potential single point failures which, if they occur could, result in:

1. extensive environmental pollution;
2. possible risk to life.

In all cases it is possible to detect the failure. In three of the four cases it is possible to initiate actions which will mitigate the effect as these failures do not affect other safety barriers.

The area of most concern is the failure of the LMV to close. This valve would only be operated should a failure have occurred in the tubing hanger resulting in the downhole safety valve failing to close. Therefore two independent failures are required before a system's safety is compromised.

Summary of critical events

The analysis of the christmas tree, LRP and surface tree has identified 65 critical events (CEs). Fifty of these CEs concern failure of the various valves in the system. These valves are required to open and close as required by the requirements of the workover rig or platform. Of these 50 failures: 28 could cause an interruption of either production or a workover, 15 could cause pollution of the environment, and 7 could lead to reduced redundancy in the system.

In all these cases the failure can be detected by monitoring of relevant system parameters and, as designed, the system, upon detection of a failure, will allow the operator to take appropriate action to reduce the effect of the failure. As part of these actions it is recommended that during a workover an ROV is readily available on the workover vessel to remotely open and close any valves as required.

Other CEs identified for the christmas tree and the riser system could result in pollution of the environment. All the events identified do not affect a safety system, so upon detection of the failure it is possible to restore the system to a safe condition.

The CEs for the surface tree are the event, which are most likely to cause loss of life due to the presence of workover rig personnel. In all cases the events can be detected and, as the safety barriers are not affected, the system can be returned to a safe state and thereby prevent extensive damage and possible loss of life.

GENERAL RECOMMENDATIONS AND CONCLUSIONS

The main recommendations of the study were that:

1. christmas tree and associated equipment should be manufactured to the specific standards, codes and approved quality assurance procedures.
2. the LMV should be tested at periodic intervals (based on manufacturer's recommendations, procedures and past experience of similar valves).
3. trained personnel should be available during normal production and/or workover mode of operation to cope with abnormal situations.

Provided the foregoing provisions are adhered to it was concluded that the subsea production system did conform to the safety requirements of DNV Guidelines 1–85 in that at least two independent failures will have to occur before a safety system is affected.

FURTHER WORK

The FMEA confirmed that the system as designed was compliant with the DNV Guidelines 1–85 with respect to safety. Although no system is completely safe the analysis had highlighted failure modes which could cause a safety related incident to occur, but two other independent failures would have to occur before any safety was compromised. In order to analyse the system further a higher level FMEA of the complete subsea production system was carried out covering the template control systems and the platform equipment. This then covered failures of other systems which could, if they occurred, affect the safety of the christmas tree.

In order to determine the probability of a combination of failures occurring, which could result in a safety related incident occurring, fault tree analysis was used. This study was outside the scope of the FMEA analysis but a review of the relevant document illustrated that all the potential failure modes which could have been considered in relation to the defined top events were covered. The overall definition of the top events had been decided as possible leak paths to the environment from the system. During the FMEA analysis various leak paths had been identified and from this initial analysis the fault trees for the system were developed. In addition, failure modes of the completion system components such as the packer were considered.

OVERALL LESSONS

The FMEA technique provided an ideal method of assessing the compliant safety of the subsea production system analysed. The technique highlighted various failure modes which would reduce the safety of the system, but these would have to be combined with other failures to compromise safety. This, though, is the main limitation of the FMEA technique. This problem can be overcome by the use of fault tree analysis on specific 'top events' highlighted in the FMEA analysis. The overall point of this is that any FMEA must be set at a realistic level in order to be worthwhile. The DNV Guidelines 1–85 provide a useful method of highlighting the failure modes identified and then assigning a probability of occurrence to the failure mode using either statistical data or engineering judgements.

Additionally, the FMEA technique provides a rigorous design tool for review of any system with regards to correct design and operation. The review of the systems specifications, which is an integral part of the FMEA technique, can easily be expanded into the design audit technique using the simple corrective action reporting forms and, where required, checklists for pertinent design points. These forms enable non-compliance with detailed technique specifications to be highlighted and appropriate action/comments recorded. The forms also allow the progress of corrective actions to be monitored both systematically and effectively. Therefore the CARF system allows the design audit technique to be expanded from the FMEA analysis in a systematic manner.

REFERENCES

1. DET NORSKE VERITAS Guideline No 1–85, 'Safety and reliability of subsea production systems', (April 1985).
2. OREDA 'Offshore reliability data handbook', 1st edition (1984).

Discussion

C J Antonakis (Ansen Ltd) Mr Lynagh is to be commended for drawing attention to the need to consider what happens if the design environmental criteria are exceeded. I have some points of issue with the author, though none of them detract from the thrust of his paper.

First, I do not agree with the definition of a '50 year wave' as given in the author's paper. My impression is that a '50 year wave' (or other event), is one which may be expected to be exceeded *at least once* in a long term average 50 years. The word 'only' in the author's paper would imply that a 100 year wave or a 500 year wave, etc could only occur once in that period. I prefer to refer to the probability number which avoids any doubts as to the meaning.

Second, a designer uses the given criteria for working within normal design stresses. In my experience he then reviews what happens to these stresses if the criteria are exceeded. If he only takes the given criteria 'at face value', he is not, in my book, an engineer.

I have not found a metocean specialist who will state the limits of confidence of his estimate of the criteria at a given place. Rather they are usually stated as 'a best estimate'. The guidance given by the Department of Energy refers to areas in fairly general terms.

Engineers do take account of the coincidence of the different events, eg wind, wave and current, and of directionality, where data are available and as far as the kinematics are understood. Such occasions are not frequent. A study made by Ansen in 1984 for the Department of Energy suggested that the cost saving that might accrue if the first generation of North Sea platforms in the UK sector had not assumed the addition of environmental forces, described by the author, may be between about 0.6 and 1.5% of the total platform cost, excluding drilling equipment and hook-up costs.

In support of the author's warning concerning exceedances, it is worth noting that the reserve of foundation strength over the imposed load for a simple gravity structure will reduce rapidly with increasing horizontal loading, and/or an increase in the height of its application. Foundation design is recognised to be an area where much caution is exercised, but until more is known about the way foundations behave, and about the extreme conditions that may be met, that caution is well merited.

Finally, there remains the problem of how to treat events of extreme rarity, but whose consequences would be severe in terms of loss of life. Until it is possible to predict when such extremes will occur it is difficult to see how the long term probability of occurrence can be used to assess what precautions to take – unless a value is placed upon a human life. Even then the amount of that value has been estimated to be anything between $1500 and $282M,[1] which seems to leave much room for argument.

Reference

1. J R Thomson, 'Engineering safety assessment, an introduction'.

N Lynagh (Noble Denton Weather Services Ltd) The definition of the '50 year extreme wave' is that wave height which can be expected to be reached or exceeded once, on average, every 50 years. This does not mean that it can be reached or exceeded only once during any particular 50 year period. Neither does it mean that it will certainly be reached or exceeded during any particular 50 year period. In fact, statistics show that there is a 63% chance of experiencing a wave equal to or exceeding the '50 year extreme wave' during an exposure of 50 years. The probability that an event with a return period of X years will be exceeded in any given duration of exposure Y years is given by:

$$\text{Probability} = 1 - (1 - 1/X)^{Y}$$

I accept the fact that an engineer will always consider what happens to stresses if the design criteria are exceeded but, from the information provided to him, what he can only guess at is by how much the criteria may be exceeded.

Metocean specialists will always state that their predictions of design criteria come into the category of 'best estimate'. It is very difficult to quantify confidence limits but as a fairly general rule I would estimate that confidence is normally no better than plus or minus 20% from the stated value. In some areas of the world where data is in short supply the confidence limits would be even wider. It is a far from exact science.

Dr P A Frieze (Advanced Mechanics & Engineering Ltd) Accepting that tropical storms (hurricanes) arise from a different population compared with the 'usual' pattern of storms, is Mr Lynagh aware of any work which seeks to generate probabilistic models representing these two events. If so, by whom?

N Lynagh (Noble Denton Weather Services Ltd) In response to Dr Frieze's question, I am not aware of any work being done to generate probabilistic models representing the two events. In general for any specific design requirements, one or other of the storm types is usually very dominant and the other can be ignored.

A R Biddle (Enterprise Oil plc)

1. In view of the fact that the new API RP2A-LRFD design methods must be more rigorous than before, it is surprising that the subjects of piles and pile sleeves have received poor treatment in Dr Frieze's paper. Is there any further work being done to correct this?
   Item 4 of the listed advantages for using LRFD methods states a more efficient use of material. Since pile steel weight can very easily amount to 50% of the jacket weight, any undue conservatism in pile design can swamp the small economies made elsewhere in jacket steel.
   In addition, if pile sleeves are conservatively designed, then this can add further steel cost and a weight penalty that could be particularly critical on lift-installed jackets.
2. It is rational to relate the load factor or resistance factor to a scale of criticality for the items involved, the criticality being judged from a sensitivity analysis. Is this being done in the API code?
3. Research work by the Steel Construction Institute on tubular frames has recently concluded that the behaviour of X joints within frames is significantly different to their behaviour when tested in isolation. Has this been incorporated in the API RP2A-LRFD code?

Dr P A Frieze (Advanced Mechanics & Engineering Ltd)

1. Mr Biddle is right to draw attention to the level of treatment of pile sleeves and piles in the preparation of RP2A-LRFD. He will be somewhat relieved to know that in the case of piles, at least, considerable progress has recently been made in quantifying the uncertainties associated with present design procedures.[1] They relate to

both axially and laterally loaded piles, and cover both clay and sand soils the former in more detail than the latter. In the case of pile sleeve connections, UK Department of Energy guidance is considered more appropriate for their design.

2. In deriving load and resistance factors via reliability analysis, it is to be expected that their values will reflect the sensitivity of design to the variable under consideration. This occurs if the associated biases are close to unity. Should biases depart significantly from unity, however, this will affect the actual level of factor finally selected.
3. API have given no direct credence to behaviour beyond first component failure in the derivation of LRFD. Consideration was given during the early phases of the work to the introduction of a system factor. However, it was not possible at the time to rationally derive an appropriate factor. Implicit allowance appears to be made for non-triangulation of structural configurations in the choice of load factors applicable to the operating conditions which is aimed, in part, at deck leg requirements. This can be interpreted as a form of allowance for system behaviour.

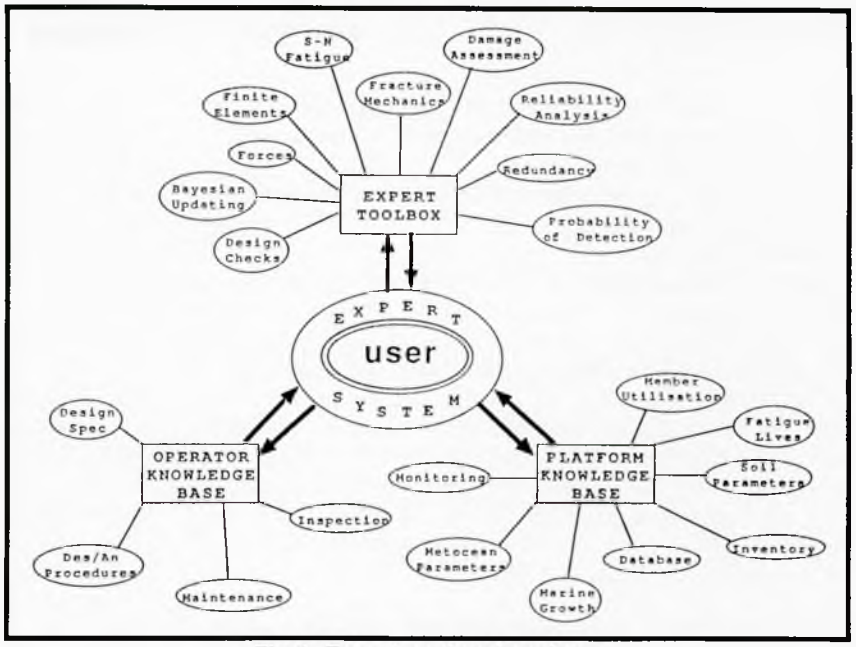

Fig 1: Expert system topology

Reference

1. W H Tank, D L Woodford and J H Pelletier, 'Performance reliability of offshore piles', Offshore Technology Conferences, Paper OTC 6379 (1990).

A R Biddle (Enterprise Oil plc) Mr Wickham and Dr Frieze have in their presentation two figures of example methodology trees by which the process of applying these techniques is explained. It would complete our notes if we would have a copy of those figures. Is this possible?

A H S Wickham and Dr P A Frieze (Advanced Mechanics & Engineering Ltd) The figures referred to by Mr Biddle relate to the PLAIM project for which the work reported in the paper forms a part thereof. As indicated in the reply to Dr Shi, this is an EC-funded project aimed at the lifetime assessment of platforms in terms of inspection and maintenance.

Figure 1 demonstrates the configuration adopted in creating the Hypercard based system described in Dr Shi's reply. Figure 2 is the more conventional 'flow-chart' form of this.

Dr W B Shi (University of Southampton) The paper by Mr Wickham and Dr Frieze is a good example of the applications of reliability analysis techniques to offshore structures.

Having read the paper briefly, I have a few comments to make:

1. On p 186, equation 24 should be written as:
   $P_{f,s} = P(E_2 \cap ... \cap E_k | E_1) \times P(E_1)$
   according to the multiplication rule of probabilities.
2. The authors' reliability analysis of the parallel system can be improved considerably but without too much additional effort.[1,2] Instead of finding a design point for each component, a joint design point for the system should be located (see Fig 3).
3. The authors' comments on how to implement the model in techno-economic analysis would be welcome.

References

1. M Hohenbichler and R Ractwitz, 'First order concepts in system reliability', *Structural Safety*, No 4, pp 267–284 (1987).
2. W B Shi, 'Technical manual for reliability analysis', NFORM, NAOE-89-49 (1989).

A H S Wickham and P A Frieze (Advanced Mechanics & Engineering Ltd)

1. Dr Shi has correctly pointed out that there is a typographical error in equation 24. It should read:
   $P_{f,s} = P[E_1 | E_2 \cap ... \cap E_k] \times P[E_2 \cap ... \cap E_k]$
   Recursive expansion of the last term leads to equation 25.
2. The identification of the so-called 'design point' for a system rather than for each component of the system is of course well known to the authors. The results presented in the paper were in fact computed using such an approach based on a Sequential Quadratic Programming algorithm. The intention of the section on the reliability analysis of parallel systems in the paper was to emphasise that system reliability analysis can, in appropriate circumstances, be performed using exactly the same set of mathematical and conceptual tools and component reliability analysis. Whether one direct identification of a system 'design point' is in fact a better way of performing a reliability analysis than the method described in that section of the paper is a moot point. Mathematical elegance and computational efficiency do not necessarily go hand in hand.
3. The terminology 'techno-economic analysis' is not necessarily widespread. Since the discussant has himself published specifically on this topic, he would be well placed to comment on the prospects for implementation of our model into such an analysis. We believe this analysis has not dissimilar objectives to PLAIM, the EC-funded project for which our model was developed. Within PLAIM, the user front-end is based on Hypercard to enable rapid location of specific sites of interest, eg a particular tubular joint. The Hypercard capabilities then allow the user to examine data bases relating to the joint dimensions, weld parameters and its specification, to its

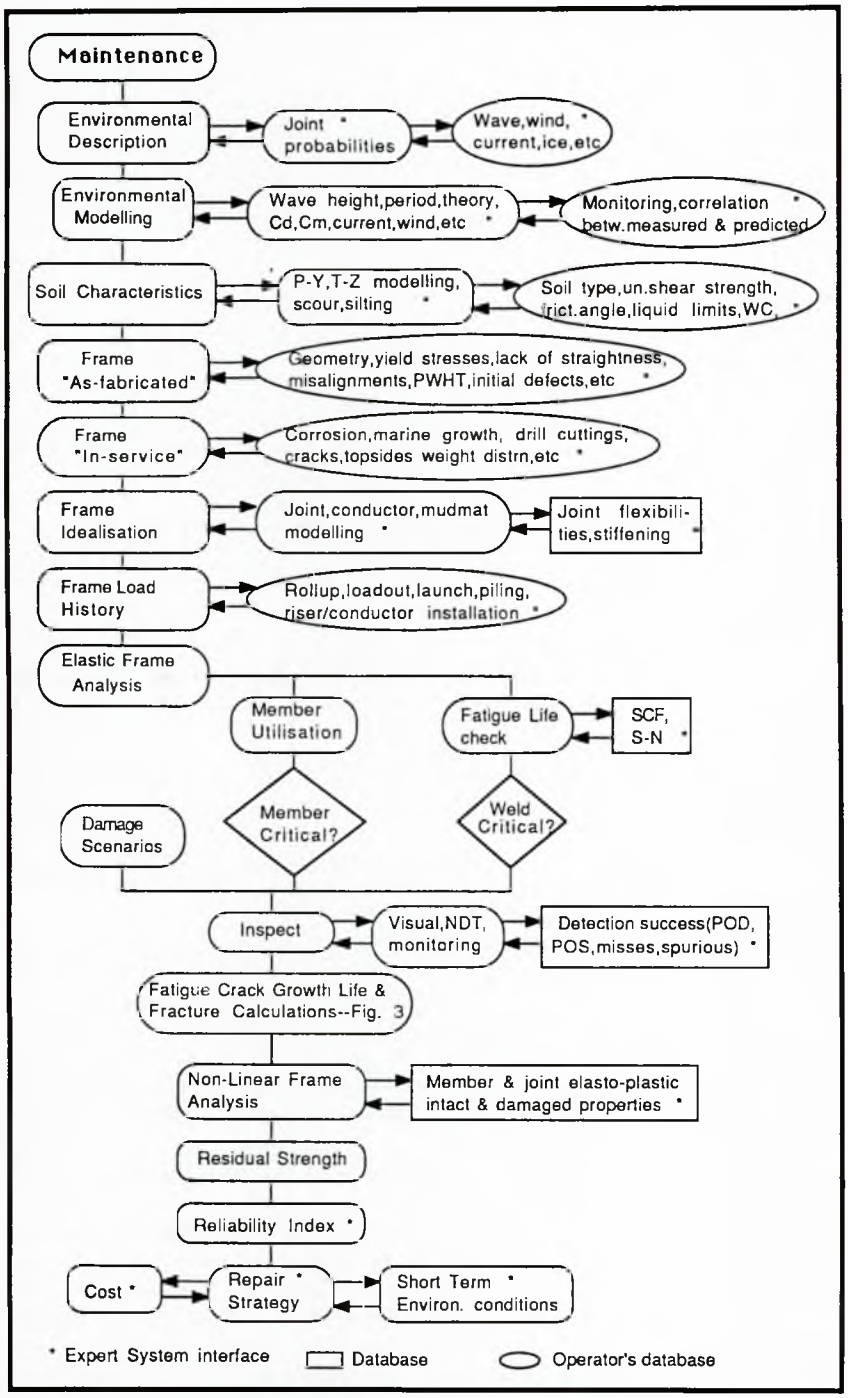

Fig 2: PLAIM strategy for platform lifetime assessment

extreme and long term load levels, its S-N fatigue life and strength, its inspection record and the detection of any cracks, defects, etc, and to algorithms for executing crack growth reliability assessment, Bayesian updating and other analyses relevant to the technological requirements of the joint. Further data bases offer repair options and their costs so that, in essence, a techno-economic analysis is possible.

The algorithms are frequently in FORTRAN which can cause interfacing problems dependent on available software. To date, we have managed to link small FORTRAN programs to Hypercard for the initiation and the retrieval of results by the latter. However, should the need arise to operate larger FORTRAN programs it will be necessary, to avoid unnecessary interruption of the front-end, to move to a far more effective multi-tasking environment than presently available to us, or to attach a slave unit for independent execution of such programs.

R H Barnes (R Barnes & Co/Ansen Ltd) The paper by Mr Deegan and Mr Burns is coincidental with the publication of the paper by Patel and Witz on the Pneumatic Compensation System in the McDermott Crane Barge DB50, formerly *ITM Challenger*.[1] I set out in the discussion to the above paper the way we tackled the FMEA of these systems, working to the American specification for Failure Modes, Effect and Criticality Analysis (FMECA).[2] Since that date (4 years ago), the British Standards Institution has published Parts of BS 5760. With DnV's rules, this gives at least three alternative procedures. Although last year I reviewed an FMEA under DnV's rules, this paper confirms one or two reservations I had then. Hopefully, this contribution is constructive and is no criticism of Mr Deegan and Mr Burns' most interesting paper.

1. *Purpose of an FMEA.* Ref 1 states that '... it is a procedure which documents all probable failures in a system within specified ground rules; determines by failure mode analysis the effect of each failure on system operation; identifies single failure points and ranks each failure according to a severity classification of failure effect ...' Also, it is a pre-requisite to carrying out a criticality analysis (CA). In summary, it is a moderating process for a design.
2. *Timeliness.* Unfortunately, FMECAs tend to have been considered by designers, contractors, customers or all three an unnecessary appendage, with the result that they have been requested late at minimum cost to satisfy some statutory requirement. As both the authors and BS 5760 state, the FMECA process can be used effectively as an audit of a design already in service.
3. *Severity levels.* For quantitative work, why not proceed logically to a formal criticality analysis if data is available, or construct a criticality matrix if it is not?
4. *Statoil and Oreda.* As Statoil's Reliability and Safety Manager is the current Chairman of the OREDA Steering Committee, I am tempted to ask whether OREDA Phase 2 data was available for this study. In particular, environmental conditions appropriate to this study are not included in the 1984 Phase 1 data but are included in Phase 2.
5. *Defining the start point.* In particular, indenture levels must be clearly defined and agreed before any start. Unless this is done at the bid stage, the consultant cannot hope to get his own costing right and may well be left with an open-ended commitment at a fixed price, if asked to delve deep into a system's guts.

6. *Novel features.* No mention was made of what must have been some novel features. Can the authors confirm this please? If so, it is probably better to work on a 'bottom-up' approach for these sections of the FMECA. The valves with duplicate seats seem to be one possible example.
7. *Diagrams.* My main criticism of the DnV rules concerns the block diagrams. There are no reliability block diagrams (RBD), drawn from functional block diagrams, to define full interdependence. These are another prerequisite to starting the analysis proper and very often show up the weakness in a system. I suggest that Fig 4, in the authors' paper, may be mistitled – blocks should be subsystems and numbered decimal fashion to prevent any confusion. This also lets the analyst know at what level he is working. Reference 3 below contains a guide to developing and drawing RBDs.
8. *Multi-function redundancy.* This is an interesting section and is somewhat similar to our own work on DB50. I set out our approach to this in an appendix to Ref 1 below. For subsystems or equipments performing two functions one could proceed as follows:
   a. Complete a matrix if and when good data become available; or
   b. Produce an effects diagram showing limitations on the end operations (Ref 1, Fig 16, p 133).

   We identified a need for continued research into reliability theory to cover multi-function redundancy of systems. Have the authors any comment to make about this?
9. *Duplication and redundancy.* This raises the old chestnut of mixing series and parallel redundancy and availability, a good example of which were the control relay failures in the Thames Barrage. Was this aspect of the study 'block diagrammed' to prevent confusion? I do agree with the fault tree approach used here, which follows BS 5760 recommendations, once an FMEA has exposed weak areas in a system.
10. *Very critical events.* The statement in item 3 of the summary of very critical events caused some concern: 'The extent of the pollution is dependent upon the extent of the failure. *If the correct operating procedures are undertaken* (my italics) the possibility of such a failure occurring will be very much reduced'. Surely are not 99%, or more, of all failures, in particular recent major catastrophes due to incorrect operation, not necessarily culpable?
11. *Assigning probabilities to failure modes.* This technique does not come across too clearly in the paper. Data is dangerous stuff and should be handled with care; Table I in the authors' paper is a gross oversimplification of the OREDA handbook and should say so. Again, pressure from clients to produce some statistics, or to show that such and such is not going to occur more frequently than something times 10^{-4} per year, can be overwhelming, if the consultant does not review available data, decide if it is relevant, and fight his corner if necessary. It is an area of serious professional concern, I suggest, to individuals working inside, or for large powerful organisations, as to the consequences of bowing to these pressures if they are present, and they are when considering novel features in systems. If good, acceptable data is available, then why not evaluate it and present it in a criticality analysis? If not, not only good judgement, as the authors' state, but also experience becomes essential, and the results can be presented on the criticality matrix.

Thank you for a most interesting and informative paper.

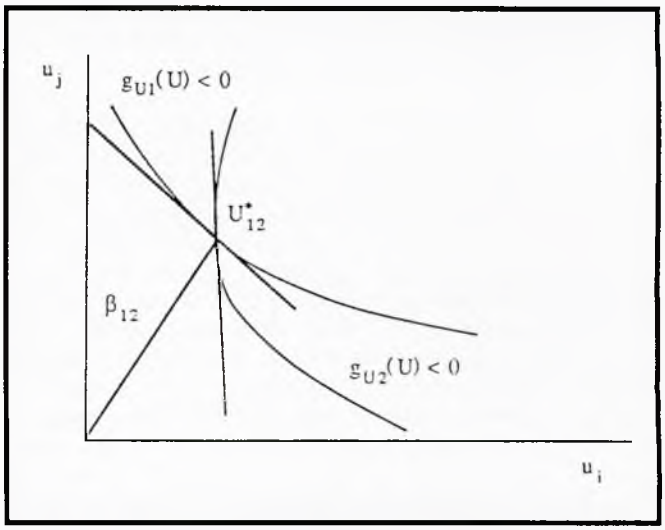

Fig 3: First order parallel system reliability analysis

References

1. Patel and Witz, 'Pneumatic compensation system in the McDermott Crane Barge DB50', *Trans RINA*, Part A, Vol 132, p130 et seq (1990).
2. 'Procedure for failure modes, effect and criticality analysis', US MIL-STD 1629A.
3. 'Reliability prediction', US MIL-STD 756.

***F J Deegan and †D J Burns (*R M Consultants and †W S Atkins Engineering Sciences Ltd)**

1. No reply is appropriate.
2. The history of this project shows FMEAs being carried out from the conceptual design stage.
3. The contract did not require a full blown criticality analysis described by MIL-STD 1629A. We did produce a criticality matrix as part of an earlier study on part of the system, but the approach was rejected after some discussion by the client.
4. The OREDA Phase 2 data was not available for this study.
5. We would most certainly agree with Mr Barnes' comments on the depth of study.
6. There were some novel features in the design. The paper presented was a composite of three stages of the work carried out. The initial phase of the work was 'bottom-up' analysis of the components of the system, ie valve components.
7. This is again the approach of MIL-STD 1629A which was not asked for by the client. In some of the literature we received from the client, RBDs of the subsystem have already been drawn.
8. A matrix of each of the component's operational phases was drawn up to allow the analyst to develop a methodology for approaching the problem.
9. No reply is appropriate.
10. No human factors analysis was asked for by the client. I would suggest though that the approach used by the Nuclear Industry, that is including human error rates in fault trees, could be used very effectively to establish the possibility of failures due to human error.
11. Some of the data in Table I of our paper has been extracted from the OREDA handbook but other data points come from in-house data sources. I would agree with the additional comment regarding the availability of suitable

data. At the end of the second phase of the work the results were presented in a criticality matrix but the methodology was rejected by the ultimate client.

***Dr D J Sherwin and †J C Bueno (*University of Birmingham and †Petrobras, Brazil)** We were very interested in Mr Deegan and Mr Burn's paper, because J C Bueno has just finished a similar exercise under D J Sherman's supervision which is currently being examined for an MPhil degree.

Messrs Deegan and Burns' analysis is restricted to mechanical failures of operation of the equipment concerned. Mr Bueno's analysis also included consideration of common cause failures. Two types of common cause can arise in this sort of equipment. The first is the (possibly environmental) event that stops everything and leads to expensive renewal or complete workover of the whole template and/or its Christmas trees, risers etc, and may cause a pollution event. The second type arises from the possibility that a common cause leads to overlapping failures of items repeated in the assembly, such as blow out preventers, and indeed whole Christmas tree assemblies. (In our case there are nine almost identical assemblies on the same template.)

Mr Bueno has developed a model for dealing with the first type which was presented in a paper (copy enclosed for authors to reply) at the Advances in Reliability Technology Symposium held at Liverpool University in April 1990. It was interesting to find that the authors, faced with a similar problem, had concluded, as we did, that fault trees were inadequate by themselves and that the FMEA could not be done (as so many are nowadays) by simply calling down existing information from a data bank into a computerised spreadsheet format, listing the standard failure modes of the components. We have come to feel very strongly that FMEA can be made a farce by such automation since seeing the same failure modes effects (and rates) listed for two electric motors, one of several megawatts and the other of 0.5 kW.

The authors are also to be congratulated upon their underplaying of the 'numbers game' in favour of careful qualitative analysis. Knowing how often something fails is little help when devising defensive or preventive measures; what matters most is *how* it fails. The roundness of the figures quoted for failure rates indicates their order of accuracy to some extent, but honest data-banks give ranges which may cover two orders of magnitude. Sensitive analysis is needed, we feel, in work of this nature, particularly if, as in our case, the environmental parameters are beyond current practice. In our study it was found that the through-life reliability (probability of no failures at all between installation and field exhaustion) was high enough at around 95% over 10 years for this to be expected system behaviour until common causes were considered, when it dropped appreciably. Even so, monitoring of parameters plus inspection by ROV, where necessary, rather than scheduled workovers (which must be by ROV), appeared to be the best maintenance policy, ie leave well alone until an incipient failure is detected because of the high cost of ROV work.

The authors are also to be praised for distinguishing so carefully the effects of various types of valve failure; stuck open, stuck shut, stuck set, leaking to environment. This led them to an equally clear distinction between operational, safety and environmental failures of the system on which they are also to be congratulated.

The authors do not refer to the extant standards covering FMEA. These are MIL-STD 1629A which is quite rigidly prescriptive and favoured by the military authorities, and BS 5760 Part 4 which is a guide to be read in conjunction with BS 5760 Part 1. This was presumably because their contract called for the use of the DNV Guidelines 1–85. BS 5760 Part 1 envisages FMEA being used initially at the feasibility study stage and then kept up to date as the design progresses. It should be used to trigger and record activities to improve the system reliability by altering the design. Too often FMEA is done as an afterthought or in reluctant compliance with contractual conditions. It is then more in the nature of an audit, since it is done too late to permit the design to be much improved. An independent analysis of a final design before it is made is a useful safeguard though, and a further audit should be carried out using real failure data from real systems in order to improve the quality of future analyses, as well as that of future similar products.

Mr Bueno's study was restricted to the underwater equipment but it did include the blowout preventers etc, and, perhaps more importantly, it considered both safety and operational time-related availability in a number of different operating modes for various numbers of wells, including oil production, gas production, water injection and also fall-back modes involving the use of gas and water lines for oil production. These considerations of flexibility prove quite important to the commercial feasibility of the project. Perhaps the authors knew more about the geology of their field and so were able to be certain of only one operational mode being needed. Ours is in deep water and there was some uncertainty about the exact geographical configuration at the time of the study, which was carried out at an earlier phase of the project.

In conclusion, we would like to say that this was a competent FMEA carried out conscientiously. It is a great pity that the powerful method is being cheapened by the application of its name to what are really no more than 'parts counts' married to standardised modes and effects analyses for supposedly standard generic system components.

***F J Deegan and †D J Burns (*R M Consultants Ltd and †W S Atkins Engineering Sciences Ltd)** We have read the paper by Dr D J Sherwin and Mr Bueno and found it to be very interesting. Common cause failures are extensively analysed in the nuclear industry but from our experience in the offshore industry they have not received the same attention. Therefore your paper is a step in the right direction.

We have read your comments on our paper and thank you for the useful criticism. The authors agree with the problems of just calling down existing data and failure modes which may be inappropriate. This is where 'engineering judgement' regarding failure modes and data is so important and 'engineering judgement' can only be gained by experience.

Regarding failure rates we, as an outside contractor, found it very difficult to obtain accurate failure rate data for some pieces of equipment as neither the manufacturers nor the operator had any historical information. That is why emphasis was placed on the qualitative approach, which we feel worked relatively well in this case.

We agree with the point regarding the stage at which an FMEA can be carried out, but it must be noted that this paper was a composite of three pieces of work. The first stage of the work was a component level FMEA of the valve assemblies and the final being the integration of all the subsystem FMEAs. Therefore, although the design audit role of the FMEA is referred to in the paper, it was only a subsidiary activity of the FMEAs in this case. In fact at an earlier stage in the design process a coarse FMEA was performed by another consultancy.

There was no water or gas injection to be incorporated in this particular field, although there were two flow lines from each Christmas tree to provide some redundancy.