

## RISK ASSESSMENT IN THE DESIGN PROCESS

V.M. Trbojevic, Four Elements Ltd., U.K; L.J. Bellamy, SAVE, The Netherlands;  
O.T. Gudmestad, W.K. Rettedal, and T. Aarum, Statoil, Norway

### AUTHOR BIOGRAPHICAL NOTES

**Dr Vladimir Trbojevic** is a Director and Manager of Offshore Oil and Gas Business Sector. He has a PhD in Finite Element techniques, and experience in risk assessment and accident dynamics. Over the past 12 years he was involved in risk analysis for improving and optimising complex engineering operations, risk analysis during design, construction to installation phases of the Sleipner A2, Troll gas and Hibernia platforms, topsides QRA in support of the Safety Cases of several platforms, and environmental risk analysis.

In the field of accident dynamics he has carried out several numerical analyses of the consequences of severe accidents such as the impact of tubular objects onto concrete platforms, where he has shown that the flexibility of the dropped object plays a more significant role than its kinetic energy.

**Dr Linda Bellamy** is a partner of the Dutch company SAVE Consulting Scientists for Industrial Safety and Senior Advisor in Safety Management and Human Factors. She has a PhD in Psychology and extensive experience in analysing the human related causes of major accidents. Over the past 15 years she has provided specialist expertise on major hazard control to chemical manufacturers, offshore operators, construction companies, maritime organisations and government departments, particularly with respect to measuring and controlling the effects of human behaviour and systems of safety management. She has led the development of techniques for integrating Human Factors into Quantitative Risk Assessment, for example for the Dutch and UK regulators and for Offshore Operators. This background resulted in her involvement in pioneering work for evaluating the human contribution to risk during the design, construction and installation phases of concrete platforms in the Norwegian sector.

**Dr Ove Tobias Gudmestad** holds a MSc degree in Applied Mathematics and a Dr Scient. Degree in Hydrodynamics. He is currently Marine Technology Advisor in Statoil and Professor of Marine Technology at Stavanger College. His fields of research interests are Wave Mechanics, Risk Analysis, Marine Technology and active engineering.

**Wenche Kristine Rettedal** holds an honours degree in Civil Engineering and Engineering Management from Glasgow University. Currently she is working in Statoil on aspects related to the basics of risk analysis. Her previous assignments have involved participation in offshore design and construction projects.

**Truls Aarum** has a MSc Degree in Civil Engineering from the Norwegian University of Science and Technology in Trondheim. He has participated in a number of offshore design and construction projects and is currently Statoil's Senior Marine Consultant to the Aasgard subsea development project.

### ABSTRACT

The detailed design phase of an offshore project is normally characterised by a very tight project schedule. There are several examples in the offshore industry of project delays and losses caused by inadequacies in the design phase. A methodology has been developed to assess the risk of the design phase of a project in order to reduce the probability for serious design errors. This methodology involves the assessment of the management of the project team, of the verification, and it requires the

cooperation of design engineers and oil company and the atmosphere of openness in the design team. It is believed that this methodology can be developed into a powerful tool to reduce the risk of design error and better channel the verification effort in future offshore projects.

The methodology for the risk assessment of the design process has been developed within the framework of Quantitative Risk Assessment (QRA). The methodology is applied in two steps: the first pass assessment combines the organisational, management and personnel system analysis which yields the error potential, which is summed with the consequence criticality of a failure in the design process to give the risk profile of the process. The results can be used in the improvement of the organisation and management of the design process, and for focusing attention for the second step, the detailed risk assessment, which combines an analysis of design task and opportunities for error into fault trees to estimate design failure probability. An example of the application of the methodology to the live design process is presented, and the benefits and practicalities of using it as a management tool discussed. Some of the intermediate findings of the analysis, expressed in the form of “strengths” and “weaknesses”, so that they can be used for risk reduction, are also given.

## **1 INTRODUCTION**

There are numerous examples of errors in engineering structures caused by faulty design. This problem has worsened as engineers rely more and more on computer models lacking old-fashioned, direct hands-on experience (Ferguson, 1993). This problem is spreading into offshore projects. The Sleipner A1 loss was, for example, partly caused by faulty finite element modelling (Jacobsen, 1992) which was undetected by the verification activities.

A major question arises as to how can one avoid catastrophic failures, or other major loss, caused by design errors. The mapping of the project organisational characteristics involving the assessment of management, cooperation, experience and verification effort is believed to be a possible way forward. This involves development of a suitable methodology for assessment of project design risk in order to arrive at organisational improvements. Many offshore projects are characterised by very hectic activities to meet the project schedule. This is particularly true for the conceptual phase where the selected concept is frozen, and for the detailed engineering phase where the effects of all possible load combinations are assessed. Errors can arise in these phases and it may be very difficult to detect them. As such it has been shown that improvements in design review of offshore jacket projects can provide substantial reliability gains with the corresponding expense being about two orders of magnitude below the cost of achieving the same result by adding steel to structures (Paté-Cornell, 1990). In order to achieve the required reliability gain, this design review must include a review of the combined conceptual and detailed design phases as well as the independent verification carried out. For a thorough discussion of verification activities in offshore projects see Rettedal et al, 1996.

A QRA-based approach was considered a useful tool to identify high risk or, safety critical elements in engineering projects. The methodology developed has been used with success for offshore construction projects (Trbojevic et al., 1994), and its merits in assessing risks during the design phase of offshore projects have been assessed (Trbojevic et al., 1995).

## **2 METHODOLOGY FOR RISK ASSESSMENT OF THE DESIGN PROCESS**

The main steps of the approach are summarised below:

### ***System Definition***

This defines the extent and the boundaries of the analysis and gives the breakdown of the design process arrangement and the organisation.

### ***Hazard Identification***

In the process of hazard identification, the critical failures of interest are those which could lead to a structural failure once the design is constructed. For example a failure in the design specification of a jacket could result in jacket failure during the application of global loads. Critical failures encompass load specification, stress analysis, material choice, documentation, and other failures. Critical failures are the direct result of:

- human errors in carrying out design tasks, and/or,
- human failure to identify a technical error in support tools like software, and
- human error in verification i.e. failure to identify errors and correct them.

In risk assessment as applied to the operating phase of an installation, the modelling of the human component of the system is typically based on the analysis of tasks of front line operators. For example, a study of dropped objects in the construction phase of Sleipner (Trbojevic et al., 1994) concentrated on the tasks of crane operators and influences on task performance when analysing human failure modes. These errors tend to be active errors (Reason, 1990), where the effects of making the error tend to be felt immediately.

By contrast, any unrecovered errors made during the design process, with a potential for causing a critical failure, will remain dormant in the system. These errors, where error occurrence is separated in time from its effects, are called latent errors (Reason, 1990). A trigger is needed for these dormant failures to become evident in the form of a near miss or an accident. Triggers include environmental conditions, atypical system states, operator errors, component failures. For example, the submergence test of the Sleipner A GBS provided the condition which triggered the latent errors in the design of the tricell. For the purpose of this methodology it is the potential for unrecovered errors which is important and not the presence of triggering conditions.

Latent errors may combine to give the potential for a major accident. Analysis of major system failures has shown the importance of this hazard in the system, and has led to descriptions of a kind of "system morbidity" such as "accident incubation" (Turner, 1978) and "resident pathogens" (Reason, 1990). In developing the methodology for design risk assessment, it is this system morbidity upon which it is important to focus, at least in the first stage of the analysis, because starting with an assessment of individual tasks at the more detailed level would ignore the important underlying sources of error.

In taking a systems view of the design process, the combining nature of latent failures can be understood in terms of organisation. The connections between the components of an organised system, the roles of each component in the system, and how they contribute to the whole have been shown to be an appropriate level of description in the analysis of major failures (Bignell and Fortune, 1984). This organisation must be viewed in the context of the climate of regulations, economic pressures, and technical know-how.

Analyses of underlying causes of failure in hazardous systems have also identified common mode sources of failure in management of a system (Bellamy, 1983, 1991). In particular, this work emphasises the importance of error recovery mechanisms and their follow up. All accidents analysed had failures in one or more of the following review and verification mechanisms which would otherwise have prevented the accident occurring: hazard reviews, inspections and audits, and checking the results of completed tasks. In design, the systems of verification/validation will be very important in recovering latent errors, and are a last line of defence against such errors remaining in the system.

The methods of human error identification and quantification (SRD, 1988) do not lend themselves well to addressing the common mode influences of organisation and management. Although one could apply human reliability assessment to the front line tasks of design (doing calculations, making drawings etc.), such an application would be enormously resource-intensive and time-consuming if key tasks to be scrutinised have not been identified beforehand. However, detailed analysis of front line tasks would be important if they were identified as contributors to areas of high risk.

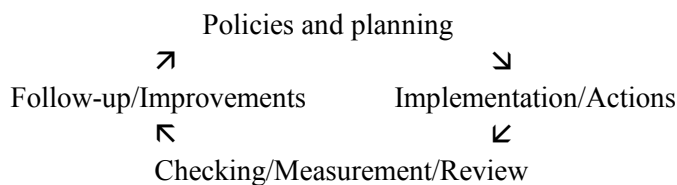
An important part of the proposed approach to risk assessment of a design process is the use of an analysis of the organisation, management and personnel system to identify areas of strengths and weaknesses in the design process which would affect the potential for these human failures. To carry out such an analysis, it is first necessary to specify the failure modes in organisation and management that could give rise to critical failures. These can be generalised to a set of sources of failure which can be summarised as:

1. Internal culture: in the design process a negative safety culture would mean not caring for the safety/quality of design outcomes, this being reflected in the beliefs, attitudes and practices of everyone involved. An example of a failure would be neglecting a safety issue in order to meet time pressures.
2. The need for control: this depends on the complexity and coupling of different organisational components of the design process which are needed in order to produce the end product. As complexity and coupling increase, so does the need for control. Therefore, failures can arise when these needs are not met, for example through failures to interface organisational units in the design flow, with the potential for different parts of the design to not “fit” with one another.
3. Possibilities for control: this covers the division and allocation of tasks, communication and coordination across organisational interfaces, ability to direct and intervene to recover errors in the design as early as possible, and the use of learning experiences from previous design projects. Failures in these areas would include: not allocating tasks to personnel with the appropriate level of competence; no way of picking up incorrect information flowing across an organisational interface; not checking or verifying key tasks, or following up key tasks which have failed the check; and not passing on information based on previous design experience to relevant members of the design team, such that the design process never improves.
4. System climate: this is the external requirements and constraints, such as economic pressures, availability of resources, and regulatory requirements which can affect safety/quality in the design process. Failures here include being susceptible to short-cutting because of failure to adequately plan for time constraints, or not ensuring there is sufficient know-how in the organisation because of unavailability of personnel resources.

The basis of the hazard identification was to develop an audit tool for assessment of the identified sources of failure in management and organisation of the design process.

### ***Estimation of Design Error Potential***

An audit approach has been taken where the strengths and weaknesses of the control and monitoring (C & M) loops of the organisation and management of the design process are assessed. The main areas addressed are based on the following control and monitoring loop concept:



The process investigates whether the loop is complete. If it is, then the investigator would expect to find:

***Policies and planning:*** The company has policies relating to safety/quality and its organisation in the design process, and there are plans or action strategies for implementing those policies.

***Implementation/actions:*** There is commitment to implementing the policies and plans. There are designated personnel with specific roles for implementing/coordinating policy and plans. There is evidence from actions that organisation for safety in design is implemented in the practices of management and front line personnel.

***Checking/measurement/review:*** The implementation of safety in design is checked by measurement, observation, reviews. This can include self checking, supervisory functions, internal auditing, third party reviews and verification/validation.

***Follow-up/improvements:*** There is a means by which the results of checks can be followed up. This means is used to improve the organisation and management of safety in design. Necessary changes in policy and planning are made.

The completeness of the loop is assessed for the four sources of failure identified previously. This is done using a tailored set of audit questions which can be scored as YES or NO based on objective evidence gathered from auditing the design process. Design error potential is then expressed on an ordinal scale, as shown in Table 1, where likelihood of error is a relative rather than an absolute value. Translating the interview results into design error potential is actually based on the translation of the "soft", linguistic variables into "hard" numerical variables (Bea, 1995).

***Excellent*** means that there are no weaknesses in the C & M loop for the organisational/task component of the design process being examined. All the question set answers would be YES.

***Poor*** means that there is effectively no C & M loop for the organisational/task component of the design process being examined. All the question set answers would be NO. In the worst possible case, the success of the task would be entirely dependent on (i) individual competence (which to a certain extent would be "luck" because the personnel selection process and allocation to tasks would

be uncontrolled) and, (ii) the "chance" favourability of the contingent conditions for task success that the personnel happen to be operating in (but which are outside their control).

The other evaluations fall in between these two anchor points. Thus:

**Good** means the C & M loop has one or two weaknesses, but is mainly strong i.e. a few NO answers to questions in random areas of the control and monitoring loop.

**Adequate** means that the C & M loop has the potential to be complete and strong. It usually, but not always, functions as intended. Those failures are not random i.e. NO answers to have some regularity and repetition in specific areas in the control and monitoring loop.

**To be improved** means that the C & M loop rarely works. Answers to questions are mostly NO.

### ***Design Error Criticality Assessment***

The term ***criticality assessment*** is used here instead of the term ***consequence analysis*** of risk assessment. Criticality assessment is one of the main tasks of the design risk assessment and its purpose is to evaluate the sensitivity of areas, components or regions of a structure to critical failures, with the potential for amplifying their effects. This assessment could be based on the QRA of the system under consideration if available, in which case the criticality is a measure of the risk variation caused by failure. This would be applicable to topsides. However, for offshore supporting structures an assessment of the reserve capacity, especially in case of the postulated component failures, is required. This is not usually available, since most of the designs are envisaged to operate in the elastic regime.

The criticality assessment for this study starts from the assumption that a particular region was under- or over-designed, leading to an assessment of the safety margins or the reserve capacity. The analysis examines the effects of a region of an offshore jacket having the load bearing capacity reduced by, say, 10% to 30%. By scanning all the regions and/or components, a profile of criticality is developed. Criticality is quantified based on severity of effects, as shown in Table 2.

## **3 APPLICATION**

### ***Organisation of the Design Process***

The methodology was applied to the design process for an important component of an offshore platform. In order to simplify the analysis, the design process was broken down into organisational units. An organisational unit is defined as a set of tasks involved in taking the input and producing the output for a single design process component. These units are shown in Table 3.

### ***Assessment***

The results of the assessment are presented in the form of "strengths" and "weaknesses" of the organisational units, some of which are listed below:

Unit 2 (characteristics: to be improved)

- There is pushing forward in the design process, with little emphasis on looking back; thus in passing on of information, there is no evidence of checking that the information was correctly interpreted and incorporated.
- There are no standards and procedures for controlling technical document content; there are only checklists.
- The design process is very people-dependent; there are systems in place (meetings, document distribution), but the process is very reliant on informal communications, and on the skills, knowledge and experience of certain individuals. There is no “organisational”, but only “individual” memory, and if key persons were to be lost from the project, it is not clear how they would be replaced, and how their “memory” would be maintained.
- The review concentrates on technical standards and regulations and meeting technical specification. There is no third party verification of the system in place (e.g. checking communications and follow-up systems, following through the flow of information, etc).
- As there are no formalised requirements for how the overall design process is organised, the review process rarely addresses whether the division and allocation of tasks is the optimal solution.
- Strong dependence of the Owner on the Verification Company for technical verification could be a weak link.
- No reference made to the functioning of TQM in the project, nor evidence put forward.

#### Unit 4 (characteristics: to be improved)

- The global model was very big and there was a reluctance to run it (or lack of resources); as a consequence of this, sensitivity analyses were not carried out.
- Certain assumptions about stress distribution derived in the conceptual (pre-engineering) stage were not checked in the detailed analysis.

#### Unit 5 (characteristics: adequate)

- Software used for post-processing was dependent upon one person.
- Development process including revisions of manuals appeared rather informal
- There were several “platform specific” versions of software in circulation.

#### Unit 6 (characteristics: adequate)

- Interface with post-processing unit was reliant on what is virtually a “black box”. It was difficult for the detailed design personnel to back check the results.
- The designers had no easy way of discovering all the assumptions made by the computer personnel who built the finite element model.

Some of the failure modes in finite element modelling, for which criticalities were assessed, are described briefly:

- Use of linear elements where more complex were recommended, or alternatively more layers of linear element should be used.
- Physical modelling encompasses potential errors in representation of loads and general assumptions in mapping the physical model into the numerical model.
- Stresses assumed compressive for the design purposes, but not checked for a combination of sub-components failures or misfits.

## ***Risk Analysis***

The evaluated risks were checked against the criteria which take the form of a matrix of error potential and consequence criticality. The potential for error (frequency) of all failure modes in the same consequence category must be added before comparison. The results of the first pass assessment are used to improve the organisational and management characteristics of all units.

Those risks which cannot be reduced in the first pass risk assessment were subjected to a more detailed analysis. The organisational unit chosen for the second pass assessment in this study was unit 4.

The probability of failure in the finite element analysis (FEA) during this component design is  $8.9 \times 10^{-3}$ , which compares well with  $3 \times 10^{-3}$  estimated for the total probability of a significant error in the FEA during the design of the "Critical Structural Details" for a class of commercial tankers (Bea, 1995). For more information on the second pass risk assessment see Trbojevic and Bellamy, 1995.

## **4 CONCLUSIONS**

The main benefits of this approach, especially of the first pass risk assessment are as follows:

- It has the capability to identify potential weak links and hot spots in a "live" design process;
- It is a "dynamic" tool for assessing the quality of the organisation and management system of the design process;
- By identifying deficiencies, remedial measures for improving organisational and management characteristics can be formulated.
- The verification effort can be focused on areas of high risk. The value of improved verification is discussed and confirmed in several studies (Paté-Cornell, 1990) where it is stated that it could decrease the probability of failure of the whole platform and thus decrease the annual probability of system failure by about 20%.
- A risk-based approach to critically assess the sensitivity of the design to the compounding effect of potential errors and to evaluate the robustness of the design is in line with the UK's Draft Offshore Installations and Wells (Design and Construction, etc) Regulations.

Potential drawbacks are:

- It requires full support of company's management because it may be misunderstood as the qualification of the management and/or personnel, making it very unpopular;
- Information gathering depends on the safety culture of the organisation, and may be a problem;
- It requires approximately 5 days of auditing and talking to the design teams (organisational units) to assess a part of the process.

The second pass risk assessment is geared more towards improving the organisation of carrying out tasks and long term management, and towards more precise assessment of criticalities, i.e. consequences of failures. Its benefits are as follows:

- The results of the detailed analysis of design tasks can be used for future planning;

- It points a way for channelling of effort where most needed;
- It will help in incorporating human reliability into future designs.

## 5 REFERENCES

Bea, R.G., "Quality, Reliability, Human and Organisational Factors in Design of Marine Structures: Approaches and Applications", Proc. of International Offshore Mechanics and Arctic Engineering Conference, Safety and Reliability Symposium, OMAE 95, Copenhagen, Denmark, 1995.

Bellamy, L.J., "Neglected Individual, Social and Organisational Factors in Human Reliability Assessment", Reliability '83, Proceedings of the 4th National Reliability Conference, Birmingham, UK, Vol.1 pp. 2B/5/1-2B/5/11, 1983.

Bellamy, L.J. and Geyer, T.A.W., "Organisational, Management and Human Factors in Quantified Risk Assessment", HSE Contract Research Report 33/1991.

Bignell, V. and Fortune, J., "Understanding Systems Failures", Manchester University Press, Manchester, UK, 1984.

Ferguson, E.S., "How Engineers Lose Touch", Invention & Technology, pp. 16-24, Winter 1993.

Health and Safety Commission, "Draft Offshore Installations and Wells (Design and Construction, etc) Regulations, 1995.

Jacobsen, B., "The Loss of Sleipner A Platform", Proc. of the Second Int. Offshore and Polar Engineering Conference, San Francisco, June 1992.

Paté-Cornell, M.E., "Organisational Aspects of Engineering System Safety: The Case of Offshore Platforms", Science, Vol. 250, pp. 1210-1217, Nov. 1990.

Reason, J., "Human Error", Cambridge University Press, Cambridge, UK, 1990.

Rettedal, W.K. Gillesvik, A., Aarum, T., Vegge, A., Kvitrud, A., "Verification of Design and Construction of Large Offshore Projects", proc. OMAE 1996, Firenze, June 1996.

Safety and Reliability Directorate, "Human Reliability Assessors Guide", SRD Report RTS 88/95Q, P. Humphreys (Ed), UK Atomic Energy Authority 1988.

Trbojevic, V.M., Bellamy, L.J., Brabazon, P.G., Gudmestad, O.T., Rettedal, W.K., "Methodology for the Analysis of Risks During the Construction and Installation Phases of an Offshore Platform", Special Issue: "Safety on offshore process installation: North Sea", J. Loss Prev. Process Ind., Volume 7, Number 4, 1994.

Trbojevic, V.M. and Bellamy, L.J., "Practicalities and Benefits of Conducting Risk Assessment of the Design Process", Conference on Assessing and Minimising Risk in the Design, Construction and Installation of Offshore Structures, Organised by IIR Ltd., London, 18/19 September, 1995.

Turner, B.A., "Man-made Disasters", Wykeham Publications (London) Ltd., London, 1978.

**TABLE 1: Design Error Potential in Relation to Evaluation of Organisation and Management Characteristics**

<b>Design Error Potential (ordinal scale)</b>	<b>Likelihood of Design Error</b>	<b>Evaluation of Organisation and Management Characteristics</b>
1	Negligible	Excellent
2	Small	Good
3	Moderate	Adequate
4	High	To be improved
5	Very high	Poor

**TABLE 2: Criticality Factors**

<b>Criticality Factor</b>	<b>Damage Category</b>
5	Total loss of the component
4	Major damage to the component
3	Minor damage to the component
2	Major damage to a sub-component
1	Minor damage to a sub-component

**TABLE 3: Organisational Units**

No.	Unit	Task
1	Pre-engineering study	Evaluation of concept and geometry envelope of the component, design loads, etc.
2	Overall organisation	Top level organisation of the design process
3	Design loads	Specification of loads and load combinations
4	Finite element analysis	Calculation of the results for the global model and unit loads
5	Post-processing	Stress calculation from FE results for load combinations and code checking
6	Detailed design	Detailed design of the component
7	Drawings	Production of drawings for the component
8	Design of sub component 1	Detailed design of sub component 1
9	Design of sub component 2	Detailed design of sub component 2
10	Assembly	Assembly of the sub components and the main component