FOREWORD

DNV is a global provider of knowledge for managing risk. Today, safe and responsible business conduct is both a license to operate and a competitive advantage. Our core competence is to identify, assess, and advise on risk management. From our leading position in certification, classification, verification, and training, we develop and apply standards and best practices. This helps our customers safely and responsibly improve their business performance. DNV is an independent organisation with dedicated risk professionals in more than 100 countries, with the purpose of safeguarding life, property and the environment.

DNV service documents consist of among others the following types of documents:

— Service Specifications. Procedural requirements.
— Standards. Technical requirements.

The Standards and Recommended Practices are offered within the following areas:

A) Qualification, Quality and Safety Methodology
B) Materials Technology
C) Structures
D) Systems
E) Special Facilities
F) Pipelines and Risers
G) Asset Operation
H) Marine Operations
J) Cleaner Energy
O) Subsea Systems
U) Unconventional Oil & Gas
CHANGES – CURRENT

General
This document supersedes DNV-RP-A203, December 2012.

Text affected by the main changes in this edition is highlighted in red colour. However, if the changes involve a whole chapter, section or sub-section, normally only the title will be in red colour.

Main changes
Definitions have been updated.
The key phrase “New Technology” is avoided in this edition, as it is not the date at which a solution is developed that governs whether or not Technology Qualification is required. The title of this Recommended Practice has been changed accordingly.

Editorial Corrections
In addition to the above stated main changes, editorial corrections may have been made.
# Recommended Practice DNV-RP-A203, July 2013

## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>D.1</td>
<td>Introduction</td>
<td>68</td>
</tr>
<tr>
<td>D.2</td>
<td>Technology Qualification Process</td>
<td>68</td>
</tr>
<tr>
<td>D.3</td>
<td>Special Topics</td>
<td>72</td>
</tr>
<tr>
<td>D.4</td>
<td>Examples of Software Reliability Analysis</td>
<td>75</td>
</tr>
<tr>
<td>E.1</td>
<td>Use of Historical Reliability Data</td>
<td>76</td>
</tr>
<tr>
<td>E.2</td>
<td>Example of extracting Data from a Database</td>
<td>77</td>
</tr>
<tr>
<td>F.1</td>
<td>Introduction to Systems-Engineering Approaches</td>
<td>78</td>
</tr>
<tr>
<td>F.2</td>
<td>A model based approach</td>
<td>79</td>
</tr>
<tr>
<td>F.3</td>
<td>Goal modelling</td>
<td>79</td>
</tr>
<tr>
<td>F.4</td>
<td>Linking evidence to leaf goals</td>
<td>79</td>
</tr>
<tr>
<td>F.5</td>
<td>Systematic elicitation of expert opinions of how well available evidence fulfils leaf goals</td>
<td>80</td>
</tr>
<tr>
<td>F.6</td>
<td>Propagation of goal fulfilment and uncertainty to overall goals</td>
<td>80</td>
</tr>
<tr>
<td>CHANGES – HISTORIC</td>
<td>81</td>
<td></td>
</tr>
</tbody>
</table>
1 Preface

The objective of this recommended practice is to provide the industry with a systematic approach to technology qualification, ensuring that the technology functions reliably within specified limits.

The approach is applicable for components, equipment and systems, which are not already covered by a Validated set of Requirements (such as an applicable standard).

**Guidance note:**
DNV Service Specification DNV-DSS-401 'Technology Qualification Management' describes how DNV can assist with technology qualification should such assistance be requested by the user of this recommended practice.

---end---of---Guidance---note---

2 Introduction

2.1 General

2.1.1 Goal of technology qualification

Technology qualification is the process of providing the evidence that a technology will function within specified operational limits with an acceptable level of confidence.

2.1.2 Motivation

Implementation of technology introduces uncertainties that imply risk for its developers, manufacturers, vendors, operators and end-users. This Recommended Practice shows how these risks can be managed by the provision of evidence to reduce uncertainties.

Concepts with well-known and proven technology are often preferred to solutions with elements of non-proven technology, even if the latter provides significant operational improvement or cost-efficiency. Technology qualification can enable its implementation, thereby helping to create new business opportunities or improve safety, reliability or profitability.

2.1.3 Objective of this Recommended Practice

The objective of this Recommended Practice is to provide a systematic approach to technology qualification in a manner that ensures traceability throughout the process, from the determination of functions, targets and expectations to relevant failure modes, qualification activities and evidence.

Its aim is to ensure that the failure modes and the qualification activities are relevant and complete. This, in turn, should improve confidence in novel technology, and improve the likelihood of its commercialisation. Thus, this Recommended Practice adds value by both facilitating the development of technology and by underpinning its business case.

2.1.4 Scope

This Recommended Practice is intended for qualification of technologies that are not covered by existing, validated requirements, and where failure poses risk to life, property or the environment, or presents financial risk.

**Guidance note:**
Even though individual components in a system might be qualified or proven, if they are assembled in a different way, the system as a whole may require to be qualified. The same applies to qualified or proven technology in a changed environment.

A process for qualification of computer software is outlined in App.D.

---end---of---Guidance---note---

This Recommended Practice can be useful for the qualification of technologies where the best way to show compliance to existing requirements or standards is not obvious.

Technology qualification is normally preceded by a concept development stage and an evaluation stage, in which the main principles for its evaluation are determined. These principles should be fed into the Technology Qualification Process via the Technology Qualification Basis (Sec.6).

2.1.5 Basis for the qualification

Novel technologies are generally not covered by established codes and procedures (validated requirements). The qualification shall therefore be based on functional specifications defined in the Technology Qualification Basis (see Sec.6).
2.1.6 Who performs qualification?
The owner, buyer, developer or a third party can perform the qualification.

2.1.7 Who benefits from the Recommended Practice?
The Recommended Practice for technology qualification serves:

— The manufacturer, who offers technology to the market and therefore needs to display proof of fitness for purpose, and/or documentation of a given technology qualification state.
— The company that integrates the technology into a larger system, and needs to evaluate the effect on the total system reliability.
— The end-user of the technology who wishes to optimise the benefits of his investment through selection between competing technologies or to create new business by doing things in an improved way.

2.1.8 Alternative methods
Alternative methods to those described in this Recommended Practice may be used providing that they are supported by equivalent evidence of the suitability of their application.

2.1.9 Structure of this Recommended Practice
This Recommended Practice is organised into two parts:

— An introduction (Sec.1 to Sec.4) in which the philosophy and principles of Technology Qualification are presented and the basic Technology Qualification Process is introduced.
— The main body containing the description of the work involved in the basic Technology Qualification Process and Technology Qualification Programmes (Sec.5 to Sec.11).

The Recommended Practice text gives options for the safest and most cost-efficient way of developing and implementing novel technology in the opinion of DNV. Supplementary advice or explanation is inserted in the text in the following way:

Guidance note:
Example of supplementary text in guidance note.

---e-n-d---o-f---G-u-i-d-a-n-c-e---n-o-t-e---

The appendices contain additional information and outline of examples and templates. The process for Technology Qualification of computer software is outlined in App.D.

2.1.10 Definitions and abbreviations
The following definitions are based on generally recognised definitions of terms as adapted to their use in this Recommended Practice.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argument</td>
<td>Demonstration of how Evidence supports a Claim in Context.</td>
</tr>
<tr>
<td>Confidence</td>
<td>In statistics, confidence is a measure of the reliability of an estimate and can be quantified by standard methods. In this Recommended Practice, the term confidence is used in a broader sense to denote the level of confidence a decision-maker has in a technology. Such confidence is usually measured when decisions are made, e.g. whether to invest in the technology or not, or implement it, or to subject it to certain qualification activities.</td>
</tr>
<tr>
<td>Context</td>
<td>Circumstances or factors relating to Technology.</td>
</tr>
<tr>
<td>Critical parameter</td>
<td>A parameter that can lead to an unacceptable level of failure, or risk, either alone or in combination with other parameters that have a similar level of risk or failure.</td>
</tr>
<tr>
<td>Element</td>
<td>The term element is used to make unspecific reference to functions or sub-functions, sub-systems or components, process sequences or operations, or execution phases.</td>
</tr>
<tr>
<td>Empirical evidence</td>
<td>Evidence accumulated through observations of phenomena that occur in the natural world, or which is established by experimentation in a laboratory or other controlled conditions.</td>
</tr>
<tr>
<td>Enhancing technology</td>
<td>A technology that provides enhanced capabilities to a user compared to existing proven technologies.</td>
</tr>
<tr>
<td>Enabling technology</td>
<td>An enabling technology is an invention or innovation that can be applied to drive radical change in the capabilities of a user. For an enabling technology there is no proven fall-back solution that can be adopted should qualification of the enabling technology fail.</td>
</tr>
<tr>
<td>Evidence</td>
<td>The evidence used for qualification includes empirical evidence, predictions using proven models and expert judgement.</td>
</tr>
<tr>
<td>Failure</td>
<td>Loss of the ability of an item to perform the required (specified) function within the limits set for its intended use. This occurs when the margin (to failure) is negative.</td>
</tr>
<tr>
<td>Failure frequency</td>
<td>The number of failures divided by the time (calendar or operational).</td>
</tr>
<tr>
<td>Failure mechanism</td>
<td>The physical, chemical, temporal or other process that leads or has led to a failure.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failure mode</td>
<td>The observed manner of failure (on a specified level).</td>
</tr>
<tr>
<td>Failure probability</td>
<td>The probability of failure occurring within a specified time period, or at a specified condition (e.g. at the start of an engine).</td>
</tr>
<tr>
<td>Function</td>
<td>A purpose for which something is designed or exists.</td>
</tr>
<tr>
<td>Functional specification</td>
<td>The performance that a technology has to achieve within set environment and operational conditions</td>
</tr>
<tr>
<td>Goal</td>
<td>The overall target of an activity</td>
</tr>
<tr>
<td>Margin (to failure)</td>
<td>The difference between the utilisation at failure and the required utilisation in the intended use. When either the utilisation at failure or the required utilisation is uncertain, so is the margin. Then the margin can be represented by its probability distribution. Performance margin and safety margin are special cases.</td>
</tr>
<tr>
<td>Milestone</td>
<td>A point in the Technology Qualification Programme that signifies an agreed qualification state has been achieved and which may be used to trigger other events such as recognition, reward and further investment (Sec.5)</td>
</tr>
<tr>
<td>Model</td>
<td>Mathematical description or experimental set-up simulating a function of the technology. Models take account of relevant effects of the critical parameters for the modelled function.</td>
</tr>
<tr>
<td>Parameter</td>
<td>A determining characteristic of the technology’s function, use or environment.</td>
</tr>
<tr>
<td>Parameter effect</td>
<td>The effects of variation of a parameter within the limits of relevance for the technology and its use.</td>
</tr>
<tr>
<td>Performance</td>
<td>The performance of a technology is its ability to provide its specified functions. These functions contribute to safety/reliability as well as the output or value generated by the system, equipment or component when in operation.</td>
</tr>
<tr>
<td>Performance margin</td>
<td>The difference between the achieved performance and the specified performance requirement. When either the achieved performance or the specified performance requirement is uncertain, so is the performance margin; in which case it can be represented by its probability distribution. Performance margin and safety margin are special cases.</td>
</tr>
<tr>
<td>Qualification activity</td>
<td>Activities aimed at providing evidence that failure modes are adequately addressed, (e.g. tests, analyses, documentation of previous experience and development of operational procedures).</td>
</tr>
<tr>
<td>Qualification phase</td>
<td>The basic technology qualification process as performed to bring the technology from one qualification-state milestone to the next milestone.</td>
</tr>
<tr>
<td>Qualification programme</td>
<td>1) Successive performance of the basic technology qualification process with incremental qualification milestones at increasing level of detail. 2) Successive performance of the basic technology qualification process for qualification with incremental improvement of the qualification limits.</td>
</tr>
<tr>
<td>Qualification team</td>
<td>The appointed team of people with relevant knowledge, skills or experience to carry out the qualification.</td>
</tr>
<tr>
<td>Qualification stage</td>
<td>1) The basic technology qualification process as performed to improve the specified limits within which the technology is qualified. 2) Technology qualification for stricter limits than the final goal.</td>
</tr>
<tr>
<td>Qualification state</td>
<td>The milestone at completion of a qualification phase.</td>
</tr>
<tr>
<td>Reliability</td>
<td>The ability of an item to perform a required function under given conditions for a given time interval or at a specified condition. In quantitative terms, it is one (1) minus the failure probability.</td>
</tr>
<tr>
<td>Risk</td>
<td>The qualitative or quantitative likelihood of an accident or unplanned event occurring, considered in conjunction with the potential consequences of such a failure. In quantitative terms, risk is the probability of a defined failure mode times its consequence, see Sec.[8.6].</td>
</tr>
</tbody>
</table>
| Risk control measure     | Those measures taken to reduce the risks to the operation of the system, and to the health and safety of personnel associated with it or in its vicinity by: — reduction in the probability of failure — mitigation of the consequences of failure  
  **Guidance note:** The usual order of preference of risk reduction measures is:  
  a) inherent safety  
  b) prevention  
  c) detection  
  d) control  
  e) mitigation  
  f) emergency response. |
<p>| Reliability              | The ability of an item to perform a required function under given conditions for a given time interval or at a specified condition. In quantitative terms, it is one (1) minus the failure probability. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety</td>
<td>The state of being safe. A technology is safe if it will not fail under foreseeable demands, leading to loss of life, injury, negative environmental impact, or unacceptable economic loss; and if it is unlikely to fail under extraordinary circumstances.</td>
</tr>
<tr>
<td>Safety margin</td>
<td>The difference between capacity and demand (e.g. load effect). When either the capacity or demand is uncertain, so is the margin. Then the margin can be represented by its probability distribution. (Special case of Performance Margin.)</td>
</tr>
<tr>
<td>Substantiate</td>
<td>To demonstrate by Evidence and Argument for a defined Context.</td>
</tr>
<tr>
<td>Technology</td>
<td>A way to provide a Function (such as by combining methods, techniques, skills, equipment, tools or materials).</td>
</tr>
<tr>
<td>Technology Qualification</td>
<td>The process of providing the evidence that technology will function within specified limits with an acceptable level of confidence. <strong>Guidance note:</strong> Technology Qualification can be seen as the process of substantiating a Claim about provision of Function, which is not covered by Validated Requirements already.</td>
</tr>
<tr>
<td>Technology Qualification Basis</td>
<td>The benchmark against which the success of the performance of the technology is measured (Sec.6).</td>
</tr>
<tr>
<td>Technology Qualification Programme</td>
<td>The framework in which the Technology Qualification Process is executed as detailed in Sec.4.</td>
</tr>
<tr>
<td>Technology Qualification Plan</td>
<td>The qualification activities specified with the purpose of generating qualification evidence and the logical dependencies between the individual pieces of qualification evidence.</td>
</tr>
<tr>
<td>Threat</td>
<td>A potential risk with significant uncertainty about the consequence of failure or likelihood of occurrence that requires further investigation to either quantify as a risk or remove from further consideration.</td>
</tr>
<tr>
<td>Uncertainty</td>
<td>A state of having limited knowledge that makes it impossible to exactly describe the existing state or future outcome(s).</td>
</tr>
<tr>
<td>Validate</td>
<td>To substantiate that something is relevant and complete.</td>
</tr>
<tr>
<td>Verification</td>
<td>Confirmation by examination and provision of objective evidence that specified requirements have been fulfilled (ISO 8402:1994).</td>
</tr>
</tbody>
</table>

The following abbreviations are used:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFD</td>
<td>Computational Fluid Dynamics</td>
</tr>
<tr>
<td>DNV</td>
<td>Det Norske Veritas</td>
</tr>
<tr>
<td>FAT</td>
<td>Factory Acceptance Test</td>
</tr>
<tr>
<td>FEM</td>
<td>Finite Element Method</td>
</tr>
<tr>
<td>FME(C)A</td>
<td>Failure Modes, Effect (and Criticality) Analysis</td>
</tr>
<tr>
<td>FT</td>
<td>Fault Tree</td>
</tr>
<tr>
<td>HAZID</td>
<td>HAZard IDentification</td>
</tr>
<tr>
<td>HAZOP</td>
<td>HAZard and OPerability study</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/Output</td>
</tr>
<tr>
<td>LCL</td>
<td>Lifetime at the acceptable Confidence Level</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure</td>
</tr>
<tr>
<td>NDT</td>
<td>Non-Destructive Testing</td>
</tr>
<tr>
<td>PFD</td>
<td>Probability of Failure on Demand</td>
</tr>
<tr>
<td>QA/QC</td>
<td>Quality Assurance/Quality Control</td>
</tr>
<tr>
<td>RAM(S)</td>
<td>Reliability, Availability, Maintainability (and Safety)</td>
</tr>
<tr>
<td>RBD</td>
<td>Reliability Block Diagram</td>
</tr>
<tr>
<td>RP</td>
<td>Recommended Practice</td>
</tr>
<tr>
<td>SHE</td>
<td>Safety, Health and Environment</td>
</tr>
<tr>
<td>SRA</td>
<td>Structural Reliability Analysis</td>
</tr>
<tr>
<td>TA</td>
<td>Technology Assessment</td>
</tr>
<tr>
<td>TQ</td>
<td>Technology Qualification</td>
</tr>
<tr>
<td>TQB</td>
<td>Technology Qualification Basis</td>
</tr>
<tr>
<td>TQP</td>
<td>Technology Qualification Plan</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level (see Appendix [B.4])</td>
</tr>
</tbody>
</table>
2.2 Technology Qualification Results and their Use

The result of the qualification is documentation of evidence that the technology meets the specified requirements for the intended use, implying:

— the probability density distribution for the service lifetime is determined and/or,
— the reliability is determined and/or
— sufficient margins are defined against specified failure modes or towards specified performance targets.

Or, in the case that the qualification efforts should fail, the result is documentation of all the collected evidence and identification of those specified requirements that were met and those that were not met using the available resources.

The qualification results can be used:

— as an acceptance for implementation of technology
— as the basis for comparing alternative technologies
— as input in the evaluation of the reliability of a larger system.
— as documentation of technology qualification state
— in documenting regulatory compliance.

2.3 Documentation Requirements and Confidentiality

2.3.1 Documentation to be provided

Documentation for the technology being qualified should contain all the information required to assess its novel aspects at a level of detail suitable for its existing stage of development. All evidence on which the qualification was based should be present. Each step of the Qualification Process should provide sufficient transparency to allow independent assessment of the qualification conclusions. All documents shall be kept up to date throughout the Qualification Process.

The documentation shall provide traceability from the qualification evidence via the qualification activities, the failure modes, the requirements in the Technology Qualification Basis, through to the qualification conclusions. It shall show the reasoning used to demonstrate fulfilment of the requirements (i.e. express the Argument).

The final set of documents normally includes following:

Technology:

— Outline of the goal.
— Functional specification.
— General arrangement drawings with position numbers related to part list and materials identification, and lay-out drawings.
— Materials specifications including documentation of their performance in the intended operating conditions and whether or not service experience in these conditions exists. This includes all information required to ensure traceability from the specifications all the way through to manufacturing and assembly.
— Detailed drawings of items subject to qualification.
— Process and instrument diagrams including control and safety systems.
— Quality assurance plan.

Documentation of the qualification shall include the following, where applicable:

Design criteria:

— References with justification to applied standards, rules and regulations.
— Reference to other criteria.

Documentation of key items in the Technology Qualification Process described in this Recommended Practice:

— The composition of the technology and evaluation of novel elements (Sec.7).
— Threat assessment including specification of personnel competence and failure mode register (Sec.8).
— List of all assumptions made in the final threat assessment.
— All qualification evidence brought into the Technology Qualification Process.
— Description and justification of methods (procedures, experience, analysis and tests) applied in the qualification activities (Sec.9).
— All results from the qualification activities.
— Documentation of resulting probabilities of, or margins to, failure modes, or margins to specified minimum performance requirements (Sec.10).
— Limiting values (maximum or minimum) for functions in the analyses and tests, such as the capacity of a pump (Sec.10).
— System reliability (Sec.11).
Manufacturing and installation:
— manufacturing and fabrication procedures
— specifications of material (including certificates as relevant)
— manufacturing records
— personnel qualification records
— installation procedures and records

Operation:
— relevant operational procedures
— service context with range of allowable environmental and operating conditions
— condition management programme with specification of intended inspection, maintenance and repair strategy and inspection and maintenance procedures.

Revisions:
— Records of all document revisions including content of revision.

2.3.2 Confidentiality
Confidentiality shall not limit the documentation from being made available for the Technology Qualification Process.

Guidance note:
It is assumed that confidentiality agreements shall be in place between parties. Scrutiny of the documentation by qualification team may follow three alternative routes:
- An open qualification scheme. This implies that all information is available to the qualification team.
- A qualification open to a third party and individual experts who are recognised by all parties involved.
- The original qualification documentation is not accessible. Full function and endurance tests according to the specifications must document the qualification, in addition to the supplier’s statement of qualification.

The latter normally implies more extensive testing. These tests shall demonstrate acceptable margins for all conditions, i.e. all applicable combinations of critical parameters. A minimum of information must be available to allow identification of the critical parameters and critical combinations in order to specify the tests. For equipment, it further implies testing of a sufficient number of units to develop statistical data and parameter effects as relevant. This method is sometimes used for electronic systems.

2.3.3 Referencing qualification evidence
The qualification shall preferably be performed with reference to generally recognised and justified standards, industry practices or specifications. For technology where there is no standard, industry practice or specification available, consideration should be given to using documents describing comparable technologies, in which case only the relevant parts shall be used and clearly referenced.

Guidance note:
Standards for “topsides” equipment and systems do not cover applications “subsea” and “down-hole”. Therefore, only relevant parts should be referenced.

If these documents fail to provide all the information needed, qualification can be based on demonstrating equivalence with those documents. In that case the requirements to which equivalence is demonstrated shall be clearly referenced. In case there is no comparable standard, industry practice or specification, qualification shall be based directly on evidence from established engineering practice, analyses and tests.

Table 2-1 lists some standards that can be applicable as qualification evidence provided that the technology is within the scope of the standard.

Further guidance for technology qualification can be found in text books in the open literature. Table 2-2 provides some examples.
2.4 Verification and Third Party Involvement

A third party is typically assigned to:

— Assess the relevance and completeness of the Technology Qualification Programme and the activities in the Technology Qualification Plan.
— Perform independent analyses and tests to verify the validity of the qualification evidence and conclusions.
— Assess and witness the Technology Qualification Process or specific analyses and tests to confirm compliance with this Recommended Practice.
— Confirm compliance with specified standards.

These verification activities shall follow a plan. This plan shall clearly identify the element of technology qualification being addressed. The verification shall be supported by a report or statement which satisfactorily covers the content of this Recommended Practice.

All elements of the technology that are considered proven shall be verified to be in compliance with validated requirements from sound engineering practices, applicable standard or performance record that demonstrates the necessary evidence.

### Table 2-1 Some standards that are applicable as qualification evidence provided that the technology is within the scope of the standard

<table>
<thead>
<tr>
<th>Id. No.</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNV-OS</td>
<td>DNV series of Offshore Standards</td>
</tr>
<tr>
<td>DNV-RP</td>
<td>DNV series of Recommended Practices</td>
</tr>
<tr>
<td>DNV Rules</td>
<td>DNV Rules for Classification</td>
</tr>
<tr>
<td>DNV CN</td>
<td>DNV series of Classification Notes</td>
</tr>
<tr>
<td>API RP 17N</td>
<td>American Petroleum Institute, Recommended Practice for Sub sea Production System reliability and Technical Risk Management, 2009</td>
</tr>
<tr>
<td>BS 5760</td>
<td>Reliability of systems, equipment and components</td>
</tr>
<tr>
<td>- Part 5</td>
<td>Guide to failure modes, effect and criticality analysis (FMEA and FMECA)</td>
</tr>
<tr>
<td>- Part 8</td>
<td>Guide to assessment of reliability of systems containing software</td>
</tr>
<tr>
<td>IEC 60300-1</td>
<td>Dependability management.</td>
</tr>
<tr>
<td>IEEE 1061</td>
<td>Institute of Electrical and Electronics Engineers, IEEE 1061, Standard for a Software Quality Metrics Methodology, 1998</td>
</tr>
<tr>
<td>ISO 14224</td>
<td>Petroleum and gas industries - Collection and exchange of reliability and maintenance data for equipment.</td>
</tr>
<tr>
<td>Z-016</td>
<td>NORSOK STANDARD, Regularity Management &amp; Reliability Technology</td>
</tr>
</tbody>
</table>

### Table 2-2 Some text books providing guidance that is useful in technology qualification

3 Technology Qualification Approach and Principles

A systems approach is implemented in this Recommended Practice to ensure that the functional specification and associated failure mechanisms are relevant and complete. The general approach shall be as follows:

— The Technology Qualification Process shall be based on a systematic, risk based approach and performed by a qualification team possessing all required competencies.
— The technology shall be screened to identify the novel elements, as these contain the most significant uncertainty. This uncertainty can be associated with the technology itself, its intended use or the intended operating environment. Qualification efforts shall focus on these novel elements.
— When uncertainties are large, iterations in the Technology Qualification Process should be performed to detect and correct for deviations.
— Possible failure modes of the technology shall be identified. Their criticality shall be determined based on their risk and preferably their contribution to the overall system risk.
— Failure modes that are not identified may pose a risk. This residual risk is mitigated by ensuring that the relevant competencies are used, by challenging mind-sets and critical assumptions during qualification (e.g. by component tests and prototype trials) and by adopting an evolutionary approach with incremental development and initial use in conditions where risk is limited.
— Elements of the technology that are not novel shall be verified separately, in compliance with a validated set of requirements (such as from an applicable standard or other specification) using the same level of scrutiny that would be applied when verifying proven technologies.
— The level of the qualification effort shall be sufficient to account for the uncertainty associated with the technology and meet the functional specification, (e.g. reliability, safety and performance). Greater uncertainty requires larger efforts or higher margins to meet a given requirement. Higher level of optimisation requires more efforts to reduce uncertainties to an acceptable level.
— When practicable, analyses shall be used to fulfil the requirements of the Technology Qualification Basis (Sec.6).
— Expert judgement used as qualification evidence shall be documented and traceable.
— Consideration of QA/QC requirements for manufacturing, assembly, installation, start-up, commissioning, inspection, repair and decommissioning of systems, equipment or components shall be covered by the qualification if these deviate from the practices given by validated sets of requirements, such as applicable standards.

The following principles govern qualification according to this Recommended Practice:

— An overall, iterative qualification strategy shall be implemented to take the technology from its existing state of development and qualification to the target qualification state, as determined by its Technology Qualification Basis.
— Specifications and requirements shall be clearly defined, quantified and documented.
— The performance margins shall be established based on recognized methods and standards, or based on the combinations of all uncertainties of the data, operation, analyses and tests.
— The qualification activities (analysis, testing, documentation of previous experience, etc.) shall aim at challenging the failure modes for the range of conditions expected in use.
— The evidence provided and the associated uncertainties shall be documented and traceable, along with the established safety and performance margins.
— Model predictions shall be verified by empirical evidence (either provided as part of the qualification or with reference to previous work).
— When service experience is used as evidence, it shall be documented and validated; the experience must be relevant and at known operating conditions/environmental conditions and must challenge the critical failure modes of the technology.
— The material, functional parameters and limits used in analyses (e.g. yield strength, friction factors, and thermal expansion coefficients) shall be based on data from tests, recognized literature or be determined by expert judgement based on such data.
— When uncertain critical parameters govern failure modes threatening life or the environment, the parameter effects shall be based on empirical evidence, and not subjective (qualitative) judgement alone.
— The qualification conclusions including any requirements to manufacturing, assembly, installation and operation of the technology shall be documented.
4 Technology Qualification Programme

The Technology Qualification Program provides a framework for managing qualification progress.

4.1 Technology Development and Qualification Progress

The uncertainties and failure probability generally decrease as a technology evolves through stages of development and as knowledge and evidence is generated through technology qualification. The Technology Qualification Process can be run throughout the development of the technology, or be started at any time in the development. Figure 4-1 illustrates that uncertainty and the probability of failure are reduced as qualification progresses, until a remaining failure probability is determined. In cases where the technology develops in parallel with the qualification activities, the uncertainty will often increase when modifications are introduced, before being reduced by further qualification activities.

![Figure 4-1](image)

Illustration of qualification progress for development phases represented by a series of milestones (MS)

The uncertainty is shown in Figure 4-1 as probability density functions. Qualification is concluded when the requirements for success, as laid down in the Technology Qualification Basis, have been reached. This process is visualised in Figure 4-1 by the probability density function of the failure margin (defined in Sec.[2.1.10]), being negative when failure occurs. Qualification concludes (success occurs) when a defined part of the tail extends below zero.

In the early stages of development, assessment of the technology depends heavily on expert judgement (often referred to as qualitative assessment). The main objective is to identify the main uncertainties. Subsequently, the Technology Qualification Process addresses the most important uncertainties and gradually replaces expert judgement with empirical evidence (often referred to as quantitative evidence). However, an element of judgements will always remain, as the reports and statements supporting the Technology Qualification Basis shall often depend on the interpretation of empirical evidence.

4.2 Contents of the Technology Qualification Programme

A Technology Qualification Program shall be established to support the management of the Technology Qualification Process. Where applicable, it shall reflect the iterative nature of technology development as illustrated in the example in Figure 4-2. The program shall also control the qualification activities and comply with steps laid down in the framework found in Figure 5-1. Elements to be included in the Technology Qualification Programme comprise:

- qualification strategy
- critical parameters
- decision gates
- the qualification team appointed to carry out the qualification
- resources needed (people, software/hardware, competencies etc.)
- roles (e.g. developer, independent reviewer, subject matter experts providing experience/analogues, independent expert consulted to enhance confidence in evidence and conclusions, providers of evidence)
- responsibilities (specify requirements, completion of work, verification, make decisions)
- involvement of stakeholders, such as partners, clients, end users, sub-contractors, authorities, third parties
- regulatory requirements
- budget constraints
- schedule and milestones
The Technology Qualification Programme should incorporate a qualification strategy that shows how the technology shall be taken from its existing stage of development to its goal. Interim milestones representing significant achievement should be established. Where possible, decision gates (at which key decisions to accept or reject a course of development, or equally invest more time and money) should be linked to the achievement/non-achievement of these milestones.

--- Guidance note: ---

This sequence of qualification development may include deployment in controlled conditions that are governed by strict limitations. Then experience from use/operation in those conditions can be used to further reduce uncertainties in a subsequent iteration by providing information on operating procedures and limitations.

Such qualification development may be facilitated by taking the technology through defined development stages such as a prototype stage where the solution is developed, a technical evaluation stage and an operational evaluation stage. Advantages in defining milestones in the Technology Qualification Programme include the measurement of progress; the review of technology qualification strategy against timelines and decision gates; and the review of technology development progress against a business plan.

It is common in the industry to use Technology Readiness Levels (TRLs, see App. [B.4]) as a means of illustrating the development stage of a technology. The TRLs (as defined in App. [B.4]) describe what broadly needs to be done to reach the subsequent level. TRLs can be used to map out the phases of a Technology Qualification Programme, providing that they include sufficient detail, including the acceptance criteria for each level.

---end---of---Guidance---note---
Qualification Basis, If it does not, a decision shall have to be made whether to adopted it as it is, (with a commensurate reduction in the Technology Qualification Basis), alter it or reject it.

**Guidance note:**
Sufficient time, effort and resources should be allocated in the Technology Qualification Plan to uncover any fundamental flaws or prohibitive obstacles as early as possible in the basic Technology Qualification Programme.

---end-of-guidance-note---

The Technology Qualification Programme is a living document that should be updated after each qualification phase to accurately reflect the status of the technology.

### 4.3 Critical Parameters List

The critical parameters list documents limits that must not be exceeded either for or by the technology. Hence, when the Technology Qualification Programme has been completed, the boundary limits for the critical parameters will represent the limits for qualification or operating envelope within which the technology is considered qualified.

Key parameters such as dimensioning loads, capacities, boundary conditions and functional requirements shall be summarised in a critical parameters list used in the Technology Qualification Process. This ensures that the relevant input parameters used for analyses and tests are updated, as changes in design or procedures are made.

The critical parameters for failure mechanisms must be identified. The critical parameters list shall include the limits/ boundaries of these parameters. Where the qualification covers a range (e.g. sizes of the product or material grades) these ranges should be defined by their respective critical parameters. For uncertain parameters, available information about the level of uncertainty should be included.

**Guidance note:**
The qualification effort can be simplified by narrowing down operational limitations, sizes considered, etc. Such limitations should then be specified in the critical parameter list. The consequences of these limitations should be assessed to see if they merit the qualification effort.

---end-of-guidance-note---

The critical parameters list should be established in the initial phase of the Technology Qualification Process. It is anticipated that both the parameters and their limits shall be refined or changed as the Technology Qualification Programme progresses and the understanding of the failure modes and mechanisms develops.

### 4.4 Qualification Team

The members of the qualification team shall be identified in the Technology Qualification Programme and their respective expertise documented. All critical areas shall be covered by the qualification team, including manufacture and end use. The expertise should also cover regulatory requirements for the technology in its intended use.

**Guidance note:**
An end user should be included in the qualification team to provide operational experience.

Care should be exercised to ensure that the team includes independent experts capable of challenging team members with vested interests.

---end-of-guidance-note---
5 The basic Technology Qualification Process

The basic Technology Qualification Process comprises the following main steps visualised in Figure 5-1:

— Technology Qualification Basis: Establish a qualification basis identifying the technology, its functions, its intended use, as well as the expectations to the technology and the qualification targets.
— Technology Assessment: Assess the technology by categorizing the degree of novelty to focus the effort where the related uncertainty is most significant and identify the key challenges and uncertainties.
— Threat Assessment: Assess threats and identify failure modes and their risks.
— Technology Qualification Plan: Develop a plan containing the qualification activities necessary to address the identified risks.
— Execution of the plan: Execute the activities specified in the Technology Qualification Plan. Evidence is collected through experience, numerical analyses and tests.

Performance Assessment: Assess whether the evidence produced meets the requirements of the Technology Qualification Basis.

Each step of the process shall be documented making the conclusions traceable. The required level of detail for documentation tends to increase as the Technology Qualification Process progresses.

Feedback loops between the steps imply that the process is iterative in nature. Consideration should be given to design modification to improve safety, performance, longevity, cost and ease of manufacture or operation, amongst others. Modification of specifications may also take place. Such modification will trigger full or partial iterations of the basic Technology Qualification Process in order for the Technology Qualification Basis to be satisfied. The need for and number of iterations will depend on factors such as:

— changes in boundary conditions
— changes to the technology (e.g. concept improvements) motivated by qualification results or external factors
— any changes needed to account for qualification results e.g. those that lie outside the specified limits (acceptance criteria)
— changes in reliability and/ or performance expectations of the technology.

Iterations shall be used to incorporate threats as they are identified; new knowledge from other qualification activities; more detailed knowledge about the technology; and capture when and how the technology has been modified. All modifications shall be identifiable and traceable and shall be reflected in the updated Technology Qualification Basis. Their impact shall be assessed against the Technology Qualification Basis. Modification to the technology shall, when relevant, have a defined purpose e.g.:
— remove a failure mode
— reduce the probability of occurrence or consequence of failure mode to an acceptable level.
— reduce the total concept cost
— improve confidence.

Modifications frequently occur due to processes outside the Technology Qualification Process such as changes in business plan or improvements in a competitor’s ability. The Technology Qualification Programme (Sec.4) should specify the interactions with these external processes.

Modifications imply that previous steps in the Technology Qualification Process need to be updated. These updates may range from the limited update of parameters or risk data, to major rework of documents based on the steps in the Technology Qualification Process. Regardless of the extent of the updates, traceability must be maintained.

Guidance note:
Modifications of a prototype will often be desirable due to the identification of unnecessary large margins for some failure mechanisms. This can lead to change in dimensional tolerances, materials selection and type of component selection. The effects of such changes must be evaluated to avoid invalidating the qualification. This will govern possible requirements for new tests or analyses.

Software can be qualified according to the same process, but since the development process for software differs from that of hardware, guidance is offered for software in App.D.
6 Technology Qualification Basis

6.1 Introduction
The purpose of the Technology Qualification Basis is to provide a common set of criteria against which all qualification activities and decisions will be assessed.

The Technology Qualification Basis shall describe the technology; define how the technology will be used; the environment in which it is intended used; specify its required functions, acceptance criteria and performance expectations. This includes the performance requirements throughout the life cycle of the technology. These requirements shall be fulfilled through the steps in the Technology Qualification Process.

6.2 Technology Description
The technology shall be unambiguously and completely described, through text, calculation data, drawings and other relevant documents. It is important that the functional description and limitations of the technology are stated and that all relevant interfaces are clearly defined. The specification shall identify all phases of the new technology’s intended life and its critical parameters.

It shall include at least the following items:

— general system description
— system functions and functional limitations
— classification and/or regulatory requirements
— standards and industry practices, or parts of them intended to be used for qualification
— main principles for storage, transportation, installation, commissioning, operation and abandonment
— maintenance and operation strategy
— boundary conditions including interfacing system requirements, environment and environmental loads and functional loads
— main principles for manufacturing and quality assurance
— relevant areas of expertise considered necessary to understand the technology
— already existing evidence claimed to support the qualification.

6.3 Performance Description
The description of performance shall be quantitative and complete.

Guidance note:
In case quantitative measures are not available for some of the performance requirements, e.g. in the early development phase, the qualification work can be carried out based on qualitative requirements, but as soon as performance requirements can be reliably quantified they should be entered into the Technology Qualification Basis and the implications evaluated.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

The Technology Qualification Basis shall express the existing technology qualification state, and the remaining milestones to complete the technology qualification. These milestones shall be laid down in quantifiable terms, e.g. be reliability requirements related to selected functions. Optionally, they may include project risk issues such as cost overrun and schedule risks.

Relevant acceptance criteria shall be specified, such as:

— Reliability, availability and maintainability targets.
— Safety, health and environment (SHE) requirements.
— Functional requirements and main data quantifying the expectations to the technology.

Reliability requirements may be specified in various forms. For medium and high-risk failure modes (Sec.[8.6]) quantitative requirements shall be specified.

Guidance note:
Examples of forms of quantitative reliability requirements are:

— The MTTF shall be larger than a specified value
— The probability of failure during a specified reference period (e.g. 20 years) shall be less than a specified value
— Equivalence to the implicit reliability level of an applicable industry practice, standard or specification.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---
7 Technology Assessment

The purpose of Technology Assessment is to determine which elements require technology qualification, and identify their key challenges and uncertainties.

7.1 Introduction

The Technology Qualification Basis forms the input to the Technology Assessment. The output is an inventory of the novel technology elements, and their main challenges and uncertainties. The Technology Assessment shall include the following steps:

— Technology composition analysis (Sec.[7.2]).
— Assessing the technology elements with respect to novelty (technology categorization, Sec.[7.3]).

Guidance note:
The novelty assessment can be complemented with an assessment of technology development stage. As an option, this can be aided by using Technology Readiness Levels (TRLs) according to the guidance provided in App. [B.4].

— Identification of the main challenges and uncertainties (Sec.[7.4]).

The input to the Technology Assessment shall be the Technology Qualification Basis. It shall be complemented by supporting documents including, but not limited to:

— detailed drawings of the items to be qualified
— drawings and description of control and safety systems
— material specifications
— outline fabrication procedures
— outline installation procedures
— outline inspection and maintenance procedures.
— existing evidence claimed to support qualification (e.g. test reports and documentation of experience).

7.2 Technology Composition Analysis

In order to fully understand the novel elements of compound technology and provide a means of communication between people with different disciplines, the technology composition shall be analysed. This is a top-down assessment that starts with the system-level functions and proceeds with decomposing the technology into elements including interfaces.

Guidance note:
Interfaces should “overlap” in order to ensure that those responsible for the different aspects of the technology or stages in its development shall understand each other.

The technology decomposition should render one or more of the following:

— Functions and sub-functions (without reference to the technical solution used to deliver the function).
— Sub-systems and components with functions.
— Process sequences or operations.
— Project execution phases, based on procedures for manufacturing, installation and operation.

Each of the elements above may include hardware and software.

The technology composition analysis shall cover all phases of the life cycle of the system, equipment or component. A goal-based analysis shall be performed to identify all relevant functions.

Guidance note:
Life cycle phases include:
- design
- fabrication and testing
- transportation and storage
- installation
- activation and commissioning
- operation and maintenance
- decommissioning
- retrieval and abandonment

A list of failure modes should preferably be established early in the development of the technology and supplemented or updated as the process progresses, including through to end of the life cycle. A list of potential failure modes is shown in App.A. This list is similar to traditional FMECA tables, but includes additional information.
7.2.1 System analysis using main functions and sub-functions

The functions are classified into main and sub-functions, with further sub-division as required.

Guidance note:
The main function is a fulfilment of the intended purpose of the technology. The sub-functions are the functions that support or add up to the main function.

Each system or equipment is analysed with respect to main functions, e.g. pumping, heat exchanging, containment, separation.

The sub-functions are necessary for the satisfactory implementation of the main function, e.g. depressurisation, shutdown process, control, containment, monitoring, start-up.

When defining both main function and sub-functions, the descriptions should provide answers to the following questions:
- When is the function started up? (Mode of operation)
- What are the characteristic modes of operation? (Actions)
- When is the problem stopped
- What is being treated, transported, monitored or stored? (Medium)
- If a process, where is the medium or energy delivered? (From - to)
- What are the performance requirements? (Requirements)

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

For complex systems, a systems engineering approach is recommended using a hierarchical structure linking the technology expectations (goals) to functions and sub-functions. At the appropriate level, sub-functions are delegated to hardware or software components. An introduction to systems engineering approaches is provided in App.F.

7.2.2 System analysis using hardware components and units

The hardware system is subdivided into sub-systems and parts, as appropriate. The main functions are delegated to these components or the interaction between them. It is essential to capture how and the level at which the main functions depend on the interfaces and interactions between the components.

7.2.3 Analysis of software composition

The software is typically subdivided into all features, capabilities, and qualities that affect the ability of the software to perform its intended function effectively. An outline of qualification of software is provided in App.D.

7.3 Technology Categorization

Novel technologies typically evolve from existing proven technologies. Normally only some elements of the technology are novel. Uncertainty is associated mainly with the novel elements. In order to focus on where uncertainty is greatest, the novelty categorization of Table 7-1 can be used. Both the novelty of the technology itself and its application area affect the uncertainty associated with the technology.

Elements categorized as novel (category 2, 3 and 4) shall be taken forward to the next step of Technology Qualification for further assessment.

Only knowledge and experience that is documented, traceable and accessible to the qualification team should be used to reduce the degree of novelty.

<table>
<thead>
<tr>
<th>Application Area</th>
<th>Degree of novelty of technology</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Proven</td>
</tr>
<tr>
<td>Known</td>
<td>1</td>
</tr>
<tr>
<td>Limited Knowledge</td>
<td>2</td>
</tr>
<tr>
<td>New</td>
<td>3</td>
</tr>
</tbody>
</table>

This categorization indicates the following:
1) No new technical uncertainties (proven technology).
2) New technical uncertainties.
3) New technical challenges.
4) Demanding new technical challenges.

This categorization applies to all of the technology being used, as well as each separate element of it. Composition analysis simplifies the identification and isolation of novel elements. The technology categorization determined shall be used to direct the qualification efforts by focusing on the degree of novelty, which shall be conservative.
Category 1 technology elements are proven with no new technical uncertainties, where proven methods for verification, tests, calculations and analysis can be used to provide the required qualification evidence. The industry practice, standard or specification validated to be applicable for each proven technology element shall be recorded in the Technology Assessment and complied with. This concludes the assessment of proven elements as part of the Technology Qualification Process. Further detailing of these elements is handled by ordinary engineering methods outside this Recommended Practice.

**Guidance note:**
Note that it is important not to overlook the proven elements, as they may be critical for the overall performance of the technology. These elements should be handled through the regular design process, ensuring compliance with an applicable standard or industry practice, implementing adequate quality assurance and quality control to ensure sound engineering design, e.g. in the form of independent design verification and fabrication follow-up. The proven elements shall then be verified according to that standard, industry practice or specification separately and verification of compliance should be done with the same level of scrutiny as if no technology qualification were involved.

Existing standards, specifications and industry standards do not fully cover novel elements. They are used in the Technology Qualification Process, however, to form a benchmark against which the Technology Qualification Basis can be set. Interfaces between the elements and external interfaces need special consideration.

Elements in category 2 to 4 require technology qualification and have an increasing degree of technical uncertainty. Elements falling into these categories shall be qualified according to the work process described in this Recommended Practice. The defined categorization makes it possible to distinguish between the novelties of the technology itself and its application areas, and focus on the areas of most concern in an iterative manner.

**Guidance note:**
Application area may refer to the experience of the operating condition, or the environment, or the purpose for which the system, equipment or component shall be used. A change in the environment, or different application of the technology, will lead to increased uncertainty. The most uncertain case is no experience in the industry for a particular application of the technology in question, in which case the category “New” would be chosen for Application Area. The least uncertain case is when there is sufficiently documented knowledge for the use of the technology element for similar conditions and applications, in which case the category “Known” would be chosen for “Application Area”.

“Novelty of the technology” refers to the technology itself. A change in any of the elements of existing technology (parts, functions, processes, subsystems) will lead to increased uncertainty resulting in selecting the technology novelty “Limited Field History” or “New or Unproven”. The change may be related to hardware or software components of the technology. Change may be related to technology elements such as new architecture configuration, system interfaces, and increased reliability requirements. The increased uncertainty may change the overall performance of the technology and its acceptance criteria.

Technology categorization does not consider the consequence of failure. As an example, category 4 may be assigned to a technology element whereas its failure may have little effect on overall system performance. If considered of value, the combination of technology categorization and consequence of failure - possibly in combination with other relevant factors for the technology - may be used to determine the technology criticality. Such criticality may be used to prioritise qualification activities.

---End of Guidance Note---

7.4 Identification of Main Challenges and Uncertainties (HAZID)

The main challenges and uncertainties related to the novel technology aspects shall be identified as part of the Technology Assessment. For complex systems, it is recommended that the main challenges and uncertainties are identified by carrying out a high level HAZID (HAZard IDentification).

**Guidance note:**
A high level HAZID is a means of improving understanding of a system at an early stage of development, and to identify which parts of the system need to be further developed or documented in more detail, prior to threat assessment.

---End of Guidance Note---

The HAZID can be carried out as a workshop, involving a panel of experts covering the necessary fields of competence and experience. The fields of expertise covered by each expert shall be documented with reference to relevant training, work experience and other relevant references.
8 Threat Assessment

The objective of this step is to identify relevant failure modes with underlying failure mechanisms for the novel technology elements, and assess the associated risks.

This is used as the basis for defining and prioritising the activities in the Technology Qualification Plan (Sec.9).

8.1 Introduction

The inputs to the threat assessment are the Technology Qualification Basis (Sec.6) and the list of the novel technology elements developed in the Technology Assessment (Sec.7). The output is a failure mode register containing all identified failure modes of concern and their associated risks. Risk is defined by the failure probability and consequence of failure as detailed in Sec.[8.6]. Its determination shall be undertaken as follows:

A failure mode assessment shall identify all possible failure modes with their underlying failure mechanisms and shall take into account each of the phases in the service life of a system, equipment or component. The failure modes shall be ranked based on their risk (defined by probability of occurrence and consequence) or their contribution to overall risk.

All failure modes shall be registered and handled using an appropriate register throughout the Technology Qualification Process, keeping track of all inputs to - and results from - the assessment, including changes, assumptions, risk category, category of technology novelty, failure probability and references to sources of evidence used in the Threat Assessment. An example is provided in App.A.

The Threat Assessment consists of the following key steps:

— Refine the technology composition assessment performed in the Technology Assessment step, if necessary.
— Define various categories of probability and consequence severity. This is done prior to the identification of failure modes.
— Define acceptable risk by constructing a risk matrix showing fully acceptable combinations (“low risk”) and unacceptable combinations (“high risk”) as well as intermediate combinations (“medium risk”) of the probability and consequence categories.
— Identify all potential failure modes and rank their risk by using the appropriate method.
— For each failure mode, rank the risk by assigning a consequence class and probability class, or by assessing their contribution to overall system risk. This can be based on previous experience, existing evidence and expert judgements. In the latter case, uncertainties shall be reflected by conservative categorization.
— Store the information for each failure mode in the failure mode register.

The Threat Assessment process can be carried out as workshops, involving a panel of experts covering the necessary fields of competences and experiences. Guidance on assessment of computer software is provided in App.D.

8.2 Refined Technology Composition Analysis

The technology composition analysis (Sec.[7.2]) shall be reviewed as part of the Threat Assessment, and refined as necessary.

8.3 Identification of Failure Modes

Expert judgement is an essential part of the Threat Assessment. Qualified personnel shall be used to identify potential failure modes, including root causes, and failure mechanism. Assessment of the probability and consequences of failure shall also be made. The experience and attainment of the qualified personnel shall be documented. The documentation shall cover all the elements covered by the failure mode evaluation.

A systematic approach for identification of possible failure modes and their related failure mechanisms shall be established and described.

Failure mode identification shall assign conservative probabilities and consequences. The updating of the probabilities and consequences shall then consider the qualification evidence and account for features such as installation, maintenance programmes and condition monitoring. Qualification evidence is discussed in Sec.9.

**Guidance note:**

This systematic can be based on traditional FMECA by individuals or in group work similar to HAZOP sessions. Group sessions might improve the identification of possible failure modes in a technology covering several technological disciplines.

To prevent the omission of compound effects caused by the assumption that mitigating actions will have taken place, it is recommended that the documentation shall clearly show the evolution of the failure modes.

In general, a failure can be identified as a failure mode, a failure cause, a failure effect, a failure mechanism, with the a root cause being traceable, see Figure 8-1.
Figure 8-1
Relationship between failure cause, mode and effect

Figure 8-1 traces the relationship between a root cause and the eventual consequences of the failure mechanism in a hardware assembly. The failure mechanism in the second column is source of the failure cause in the third column. The failure effect on the seal, sub unit (pump) and equipment (pump with instruments lubrication) is shown in each of the levels. Such system decomposition shall be performed down to the level of the critical failure mechanisms. This enables a systematic check of the margin to failure as covered by Sec.9. These relations are documented in a Failure Mode Effect Analysis (FMEA) as shown in App.A.

References for FMEA/FMECA:
- BS 5760, Part 5, Guide to failure modes, effects and criticality analysis

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

8.3.1 Threat assessment methods

There are several threat or failure mode identification techniques in common use. The selection of method should take into consideration the complexity and maturity of the compound technology. The threat assessment shall cover all novel elements defined in the technology composition analysis. The output is a record (failure mode register) of all identified failure modes, failure mechanisms, consequences and probabilities and their associated risk. Various methods for risk analysis can be used for the Threat Assessment. Table 8-1 lists some of the advantages and disadvantages of different methods.

| Table 8-1 Advantages and disadvantages with different threat assessment methods |
|-------------------------------------------------|-------------------|-----------------------------|
| Method                                         | Advantages         | Challenges and/or Disadvantages |
| Failure Mode, Effect and Criticality Analysis (FMECA) | Systematic and simple to apply | Investigating ONE failure mode at a time may not identify critical combinations of failures |
| Hazard and Operability study (HAZOP)            | Systematic method which enables identification of the hazard potential of operation outside the design intention or malfunction of individual items | Resource consuming Requires detailed information for producing useful results. Experienced facilitator required |
| Fault Tree Analysis (FTA)                      | Thorough investigation of (already) identified incident | Not applicable for identifying (new) incidents. Time consuming to set up Not suitable for accurately modelling all types of systems |
| Structured what-if checklist (SWIFT)            | Applicable even if detailed design information is not available | Experienced facilitator essential, as well as good checklists |
| Operational Problem Analysis (OPERA)            | Emphasis on the product interfaces | Emphasis on technical problems and human error without going into details about causes |
| Independent review                              | Can be more time efficient or less resource demanding | Not as multidisciplinary and robust as other techniques |
8.4 Consequence of Failure

Consequences of failure shall, when relevant, be detailed for:

— the functions of the technology itself
— impact on surrounding and interfacing systems
— operation and repair
— safety, health and environment (SHE).

It is recommended that these consequences are recorded as estimates of monetary loss, as this tends to help the qualification team relate the magnitude of the risks to the cost and practicability of their mitigation.

**Guidance note:**

One way to categorise the consequence groups is as follows:

**Consequence for novel technology:**
- insignificant
- reduced part of main function
- loss of parts of main function
- loss of main function
- loss of main function and damage to interfacing and surrounding systems.

**Consequences for surrounding and interfacing system:**
- no effect on interfacing and surrounding systems
- insignificant effect on interfacing and surrounding systems
- shutdown of interfacing and surrounding systems
- noticeable damage to interfacing and surrounding system
- severe damage to interfacing and surrounding system.

Further economic consequences are:
- lost production
- repair options and spare parts
- mobilisation and repair time
- damage to reputation/brand.

Each of the above economic consequences affects budget and timeline. Determining monetary consequences enables cost estimates to be made. This can help trigger design revisions, which would be more expensive to resolve later. Selection of a typical sample installation is beneficial for providing a cost example. Cost varies over time and location. As an example, for deep water and subsea well systems, the cost of the vessel hire will normally dominate.

The consequence classes for the SHE area are normally:
- Health & Safety – potential for personnel injuries and fatalities.
- Environment – potential for environmental effects.

An example of overall consequence classes is provided in Table 8-2. The effect of including additional consequence categories to those related to safety (e.g. delay/downtime and reputation) is that the Qualification Process can define qualification activities to account for these aspects that come in addition to those activities needed to account for safety.

Consequence classes shall be chosen in each individual failure mode using expert judgement and experience. This shall be done for the system as specified without account of any proposed safeguards that have not yet been adopted and specified.

**Guidance note:**

The following generic example of qualitative consequence classes in Table 8-2 is shown for illustration only and must not be adopted without assessing applicability to the particular case and its intended use and operating environment.
In Table 8-2, the number of defined classes has been reduced by combining several types of consequences into one set of classes. A single class represents specific consequences for people, environment, delay/downtime and/or reputation. Within one consequence class, the consequences of all types have been defined in order to represent similar levels of severity.

It is important that for a particular event with more than one type of impact, the type of impact giving the highest class shall be governing the single consequence class.

--- end of Guidance note ---

8.5 Probability of Failure

8.5.1 General

Probability of failure shall be established for each failure mode. The early technology development phases (concept) could use qualitative measures. As the Technology Qualification Process progresses, quantitative evidence should be collected in order to demonstrate that the Technology Qualification Basis has been met.

Guidance note:
This demonstration may take the form of describing the failure modes by their lifetime probability-density distributions, or by showing that established standards or specifications have been used, or that sound engineering practice has been followed. Methods for documenting quantitative failure probability are discussed in Sec. [9.6].

--- end of Guidance note ---

Documentation of quantitative failure probability shall be based on evidence such as:

- test results
- numerical analysis based on recognised methods
- relevant, documented experience
- engineering judgement by qualified personnel.

If evidence supporting failure probability estimates is lacking, conservative estimates shall be established. The degree of conservatism shall reflect the level of uncertainty and hence increase with novelty (category 2 to 4). The conservatism of assumptions shall be substantiated.

The estimated probability of a failure mode shall be split in failure probabilities related to each identified failure mechanism, see Figure 8-1.

Normally the probability would be expressed as:

- probability within service life, or per year of operation
- probability on system activation
- probability distribution for the lifetime of the system.

For risk-ranking, a direct probability assessment can be used, i.e. reliability judgement by qualified personnel. Expert judgments should also be applied during planning and gathering of reliability data to assess relevance, and possibly suggest adjustments of evidence based on partially relevant data, in order to account for differences in relation to the system to be qualified.

It is important to avoid biases that in general may be easily introduced when dealing with expert opinions.

Guidance note:
Guidance on expert elicitation and how to deal with subjective opinions in reliability in general can be found in the open literature, e.g. Cook (1991).
Expectations for target failure probability based on engineering judgement and information from databases are commonly used in the initial development phases. The offshore industry often utilises the following databases in the initial phase, before a failure probability has been proven by actual experience, analysis or test:


WELLMASTER – Reliability of Well Completion Equipment. Data can be made available on an electronic format via the following Internet address: http://www.exprosoft.com/products/wellmaster.html.

SUB SEA MASTER – Reliability of Sub sea Equipment. Data can be made available on an electronic format via the following Internet address: http://www.exprosoft.com/products/subseamaster.html.


Further databases are:

HRD4, BRITISH TELECOMMUNICATIONS PLC. Handbook of reliability, Ascot: London Information (Rowse Muir).

Failure probability based on information from databases often needs adjustments before being applied to new systems, different use, different environment etc. An example of such adjustment is illustrated in Table 8-3. It is of utmost importance to understand and identify whether the reported data in the database can be used to represent the technology, or if some failure modes may be incorrectly represented due to differences in use.

The failure probability based on such general databases or expert judgement should be updated based on tests or documentation in the later phases of the Technology Qualification Process.

<table>
<thead>
<tr>
<th>Sub-component</th>
<th>Reference data</th>
<th>Data qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Penetrator</td>
<td>5</td>
<td>0.50</td>
</tr>
<tr>
<td>Cooling system</td>
<td>3</td>
<td>0.30</td>
</tr>
<tr>
<td>Winding</td>
<td>6</td>
<td>0.60</td>
</tr>
<tr>
<td>Switch</td>
<td>2</td>
<td>0.20</td>
</tr>
<tr>
<td>Other</td>
<td>10</td>
<td>1.00</td>
</tr>
<tr>
<td>Total</td>
<td>26</td>
<td>2.60</td>
</tr>
</tbody>
</table>

Failure frequency per 10^6 hrs

---end---of---Guidance---note---

### 8.5.2 Qualitative probability classes

Qualitative probability classes may be used to establish failure probability in early development phases. The classes must be chosen in each individual case using expert judgement and previous experience.

**Guidance note:**
Table 8-4 shows an example of generic qualitative probability classes.

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Failure is not expected ( (p_f &lt; 10^{-4}) )</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>An incident has occurred in industry or related industry ( (10^{-4} &lt; p_f &lt; 10^{-3}) )</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Has been experienced by most operators ( (10^{-3} &lt; p_f &lt; 10^{-2}) )</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Occurs several times per year per operator ( (10^{-2} &lt; p_f &lt; 10^{-1}) )</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Occurs several times per year per facility ( (10^{-1} &lt; p_f) )</td>
<td></td>
</tr>
</tbody>
</table>

---end---of---Guidance---note---

### 8.6 Risk Assessment

A qualitative method to determine the risk level can be used in order to rank risk and focus qualification efforts where the benefits are greatest. The risks are categorized as illustrated in Figure 8-2. The risk categorization should be adapted to fit the case being considered. The adapted matrix shall govern the Technology Qualification Plan with respect to priority, with focus on the highest risk. It shall define high consequence risks as medium or high risk, regardless of probability class, to ensure that high–consequence/low-probability risks are addressed by the qualification activities and not dismissed, based on low probability.
The failure modes are ranked according to risk category. Failure modes with medium and high risk are considered **critical** and shall be covered by the Technology Qualification Plan (Sec.9). Failure modes with low risk can be concluded based on qualitative assessment by qualified personnel. Failure modes with low risk shall not be deleted from the list of possible failure modes.

The risk estimates shall be updated during the Technology Qualification Process, utilising qualification evidence and information from mitigating actions that become available through the Technology Qualification Process.

The risk assessment shall be performed at the level of detail relevant for the respective development phase. A system for tracking each failure mode and failure mechanism shall be established (an example is shown in App.A). The purpose of this system is to maintain traceability back to each failure mode and mechanism, from identification, through change, to the verification that the risk has been addressed as the Technology Qualification Process is followed. This system shall include:

1) All identified failure modes and mechanisms.
2) Probability estimate for each failure mode/mechanism.
3) Basis for the probability estimate, tracing documentation revisions and implementation of mitigating actions.
4) The degree of novelty to which the failure mode relates (category 2 to 4). This aids focus on the novel elements.

### Figure 8-2
**Risk matrix; L=Low, M=Medium, H=High**

<table>
<thead>
<tr>
<th>Increasing severity</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>2</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>3</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>4</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>5</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>

Increasing likelihood
9 Technology Qualification Plan

A Technology Qualification Plan shall be developed to provide the evidence needed to manage the critical failure modes identified according to Sec.[8.6]. The development of the Technology Qualification Plan should be an iterative process.

9.1 Introduction

The selected qualification methods shall be specified as activities in the Technology Qualification Plan. A qualification method shall be described in sufficient detail to carry out the activities and obtain reliable evidence. These activities provide evidence to document compliance with the requirements of the Qualification Basis. The qualification activities shall be traceable back to the failure mode register developed during threat assessment. The reasoning relating the pieces of evidence to the failure modes shall be presented.

Guidance note:
An example plan for qualification of a subsea booster pump is shown in App.C.
For components produced in large numbers and used in different types of systems, the need for standardisation and thereby cost reduction often governs the qualification strategy, as indicated in App.C.

The following sub-sections address various aspects to be considered in the specification of qualification activities.

The Technology Qualification Plan should reflect the iterative nature of the overall qualification strategy (Sec.4) and of the basic Technology Qualification Process (Sec.5), seeking to reduce the largest uncertainties first. An overall Milestone Plan is recommended to reflect the chosen strategy towards the overall goals.
Detailed plans should be developed for a reasonable period (e.g. until attainment of the next major milestone).
The major milestones should be concluded with an independent review.

Development of the Technology Qualification Plan consists of the following main activities:

— High-level planning to implement the overall qualification strategy.
— Analysis and selection of qualification methods to provide the evidence needed for each failure mode.
— Develop the reasoning that connects the evidence produced by the qualification methods to the requirements set in the Technology Qualification Basis.
— Develop detailed specifications of qualification activities.

The detailed specification of qualification activities shall explicitly specify:

— The evidence to be produced by each qualification activity.
— The failure modes each piece of evidence relates to. (Argument.)
— The reasoning that relates the pieces of evidence to the failure modes. (Argument.)
— The reasoning that relates the evidence to the requirements specified in the Technology Qualification Basis (Argument.).
— Success criteria for this evidence in meeting the requirements. (Context.)

The Technology Qualification Plan shall be revised as necessary. When the technology has been successfully demonstrated to have reached a major milestone, detailed plans can be developed for reaching the next major milestone accounting for what has been learnt.

Guidance note:
The choice of methods to achieve qualification will depend on the nature of the requirements stated in the Technology Qualification Basis. For instance, reliability targets require quantitative reliability prediction; and the methods to generate data will depend upon the type of required input.

9.2 Selection of Qualification Methods

Qualification methods shall be specified that provide evidence for each identified failure mode, showing that the requirements stated in the Technology Qualification Basis have been met.

If a quantitative reliability target is stated in the Technology Qualification Basis, then a quantitative reliability method is required to document fulfilment of the target, e.g. by determination of a lifetime probability density distribution for the relevant failure modes.

For each failure mode of concern, it should be determined if the failure mechanisms can be modelled by recognized and generally accepted methods. Then a detailed plan for the qualification activities can be established by use of existing standards, specifications or recognised industry practices that have been validated for applicability.
The following methods can be used, separately or in combination, to provide qualification evidence:

— Analysis/ engineering judgement of previous, documented experience with similar equipment and operating conditions.
— Analytical methods such as handbook solutions, methods from existing standards, empirical correlations or mathematical formulae.
— Numerical methods, such as process simulation models, CFD, FEM, corrosion models, etc.
— Experimental methods as discussed in Sec.[9.4].
— Inspections to ascertain that specifications are complied with or assumptions valid.
— Development of new or modified QA/QC requirements for manufacturing / assembly.
— Development of requirements to inspection, maintenance and repair.
— Development of operating procedures resulting from the Technology Qualification Process.

**Guidance note:**
Operational procedures are important elements of a reliable technology. They must be documented and implemented when the technology is deployed. Implementation should cover the entire supply chain and receiving organisation.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

— Developing modifications to the technology arising from the above that would spawn a new iteration in the technology qualification/development cycle.

**Guidance note:**
The selection of qualification methods and required scope depends on the risk of the associated failure mode, technology category, and level of confidence in the methods. The objective is to specify a Technology Qualification Plan that provides the most reliable evidence as cost-effectively as possible. The selection of the methods should therefore be based on optimization of related cost versus accuracy. Each qualification method can address several failure modes. Thus, the methods should be selected in a systematic manner to reduce unnecessary overlapping.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

Alternative methods should be considered for the most expensive qualification evidence.

**Guidance note:**

1) Least cost will mainly be obtained by the use of thorough, theoretical analytical models. Subsequent uncertainties can be focused and resolved by optimised tests. (The alternative would be more extensive tests to determine dependencies and failure modes.)

2) It would normally be beneficial for manufacturers to standardise the qualification scheme for small components. Thereby the margins for some applications may be unnecessarily high, but justified by the total cost reduction, e.g.: pipe fittings or electronic components).

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

**9.3 Parameter Effects and Models**
The qualification activities must account for the effects of uncertainties in the critical parameters (parameter effects).

If a proven numerical or analytical model exists to simulate a failure mechanism in the intended environment, that model can be used to assess the parameter effects associated with that failure mechanism.

If confidence is lacking in the available model, it must be proven by tests to validate the predictions in the relevant parameter range covering short-term and long-term behaviour.

If no applicable model exists for the parameter effects then it can be developed. The validity of the new model shall be proven through qualification activities.

The proven numerical or analytical model shall be used to establish the parameters with the highest impact on the lifetime and reliability of the technology.

The following model-based qualification approach shall be reflected in the Technology Qualification Plan:

— Utilise or develop models of the critical failure modes using, to the extent possible, models that have been proven.
— Identify uncertainties in the models and model input data.
— Characterize input data for models with the associated uncertainty.
— Build confidence in the models. This is achieved through qualification activities that challenge them by comparing model predictions with relevant evidence, e.g. from experiments performed as part of the qualification, published data or service experience.
— Use model to quantify parameter effects.

**Guidance note:**
Service experience from other industries may be validated to be relevant and hence used as basis for building confidence in qualification models.
Guidance note:
There exists a range of analytical models of failure mechanisms. Some methods are suited to predicting the probability of occurrence of the critical failure mechanism. Other analytical methods can not directly predict a failure probability. However, if the method is empirically justified to relate to probability - and is generally recognised and accepted - a correct application of the method can be used to determine a failure probability.

An example of such analytical methods is mechanical stress calculation methods used for pressure vessels according to a pressure vessel standard. Provided there are no material deterioration or fatigue mechanisms, stress calculated to be below the acceptance criterion assures a safe pressure vessel within the standard’s limitation, and hence a probability of failure less or equal to that defined or implied by the standard. In this case, the pressure vessel can be taken to have the failure probability specified in, or implied by the standard. Failure mechanisms related to design, manufacturing, application and accidents, however, are possible sources of failure that also need to be taken into account. These probabilities may be reduced by quality control, verification activities, and operational procedures. The effects of such mitigating actions can be included based on documented experience or engineering judgement.

In case a reasonable model cannot be established, the parameter effects can be established by qualification tests (Sec. [9.4]).

When applicable, conservative expert judgement based on empirical data may be used to establish the critical parameter effects for the failure mechanisms. An example is provided in Appendix [C.2]. Expert judgement requires qualified personnel.

For the analysis of software reliability, specific methods apply (see App.D).

The system sensitivity to uncertainties of the critical parameters shall be established, and the critical parameters list updated.

Uncertainties in numerical calculations shall be estimated based on the possible uncertainties in the:

— input parameters
— analytical method
— result presentation.

The resulting uncertainty of the analysis shall be determined based on recognised methods.

Guidance note:
Temperature is an example of a common cause of uncertainty. The temperature could affect each part in a measurement set-up the same direction and thereby cause a larger error than assumed.

9.4 Experimental Methods
Experiments are an essential part of most qualifications, and aim to provide the experimental evidence on which qualification is based.

9.4.1 General
The extent of the experimental tests required to obtain qualification evidence for the technology depends on the technology type, confidence in analyses, the level of optimisation aimed for, and the extent of documented experience with similar technology. The test programme shall specify:

— The tests to be carried out.
— The purpose of each test with reference to the targeted failure modes and requirements in the Technology Qualification Basis.
— Acceptance criteria for the results in order to meet the targeted requirements.
— Limiting values for design of the test (e.g. maximum load).
— The parameters to be measured and recorded.
— The accuracy requirements to measurements.
— The method of analysis of the recorded data.
— The reasoning that relates the data to the failure modes and the requirements specified in the Technology Qualification Basis.

Experiments/ tests shall be planned as part of the qualification. The purpose of qualification tests can be to:

1) Explore novel elements of the technology, and help identify failure modes and mechanisms of relevance.
2) Provide empirical evidence for functionality and reliability assessment.
3) Identify or verify the critical parameters and their sensitivities.
4) Characterise input parameters for models.
5) Challenge model predictions of failure mechanisms. To challenge the models, the tests should cover extreme values of the critical parameters with respect to the qualification basis.
Recommended Practice DNV-RP-A203, July 2013
Sec.9 Technology Qualification Plan – Page 32

These qualification tests form the basis for - and determine the outcome of - the qualification. Technology qualification may also specify tests to be performed after qualification is completed as a condition for deploying the technology. This is discussed in Sec.[9.4.4].

Each qualification test shall be designed to meet a particular need arising from the technology qualification. Traceability via identified failure modes to requirements specified in the Technology Qualification Basis shall be provided. If a standardised test is identified that addresses a similar issue, its relevance for the qualification needs shall be validated. The standardised test shall be amended or redesigned if it does not satisfy the qualification needs.

Guidance note:
Standardised tests are developed for a need that existed when the test standard was written, inevitably in relation to a technology that existed at that time. Rarely are these tests equally well suited to novel technologies. It is a common mistake in technology qualification to use a particular test merely because it is standardised, and thereby failing to address the qualification needs properly.

Accelerated tests can reduce test time and cost. Such tests are beneficial when a proven parameter model exists and the uncertainty of model predictions established. It is a common mistake to rely on accelerated test methods that are not proven.

---end---of---Guidance---note---

Confidence in the experimental evidence shall be ensured by independent review of test specifications, including instrumentation and quality assurance of the test activities, and independent witnessing of tests as appropriate.

The accuracy tolerance of each measurement result shall be established based on a list of the uncertainty for each component. This may affect the required:

— calibration accuracy
— sensor accuracy
— signal processing accuracy
— recording accuracy
— reading accuracy.

9.4.2 Characterisation tests

Characterisation tests determine the inputs to the qualification models. These tests shall establish the key parameters to be used in the design, when they are not available in recognised and accepted literature, or from documented experience.

Guidance note:
Examples include material characterisation tests that are used to estimate the material properties (including their uncertainty), tests to characterise the chemical reactivity of substances used in the technology, and ageing tests used to estimate how such basic properties develop with time under controlled conditions.

---end---of---Guidance---note---

9.4.3 Component tests and prototype tests

Prototypes of components, equipment or systems may be subjected to experimental evaluation either in a laboratory or in trials in controlled situations where risks can be managed.

The requirements specified in the Technology Qualification Basis shall be used with the corresponding failure modes to determine success criteria for component and prototype tests. Testing to failure is the only way to directly measure the margin to failure; and testing to failure greatly enhances the value of the test compared to a functionality test that only provides evidence of no failure at the tested conditions.

In the early phases of qualification, the purpose of component and prototype tests can be to explore novel elements of the technology, and help identify relevant failure modes and mechanisms, or explore the critical parameters and their effects. If models are developed as part of the qualification, they need to account for the critical parameters.

Another purpose of component and prototype tests is to challenge model predictions. Recordings of responses and failures in the tests provide strong basis for comparison with model predictions.

Provided that the test conditions are sufficiently close to the intended service conditions, such tests can be regarded as physical models that directly provide evidence of the performance of the technology. If sufficient tests can be afforded to provide statistically significant estimates of the behaviour of the technology, such tests can alone constitute the evidence required for the corresponding failure mode.

Component and prototype tests can often not be afforded in sufficient numbers. The value of limited tests can be improved concentrating to validation of models. If validation is successful, then the model may be included in the qualification evidence. Disagreement between model prediction and experimental evidence should spawn new qualification activities (iterations) to resolve the disagreement.
Prototype and component tests are recommended to provide assurance against potential unidentified failure modes, particularly if materials are novel or used in environments where relevant service experience is lacking. Test items shall be produced using the same raw materials and components, according to the same manufacturing procedures, and to the same quality standards as specified for use in the actual production unless these aspects are assessed specifically, and documentation is provided that the test item is safe, representative and conservative for its purpose or period of use. The actual tolerances achieved for all critical parameters shall be recorded for each test item. Materials review and manufacturing reviews shall be planned to ensure that the test objects are in accordance with specifications.

For cases with acceptable failure consequences, verification can be obtained in actual service as an alternative to prototype tests.

9.4.4 Other tests

The technology qualification may identify certain conditional tests on as-produced products to meet certain acceptance criteria. As such they are not qualification tests. Examples include:

1) Quality assurance tests performed during manufacturing after the involved technologies have been qualified that confirms compliance with the conclusions from the qualification.
2) Factory acceptance tests (FAT) prior to each delivery as a quality assurance measure to reduce the probability that defects slip through to service.
3) Pre and post installation tests of the full assembly to verify the soundness prior to and after the completed installation.
4) Pilot application represents the first use, and can therefore be planned as an advanced test to gain more experience with the system, ensuring that all aspects of a complex system has been taken into account.
5) Tests to be done as part of maintenance to confirm that the qualification conditions are maintained during service (such as NDT) etc.

An essential part of the Technology Qualification Process is to specify these tests and the acceptance criteria for implementation of the technology.

The purpose of such tests is to provide evidence to verify that the final product complies with the assumptions of the technology qualification. Non-conformance requires rejection of specific product, modifications to the equipment or re-qualification to changed conditions.

However, when performed after concluding the qualification, these tests produce evidence that may be relevant for the qualification status. Such evidence may be taken into a re-qualification that may lead to changes in the operational envelope, test requirements, or maintenance and inspection requirements. When intended used for this purpose, these tests shall be carefully designed to challenge the model predictions used as basis for qualification or to challenge specific failure mechanisms.

Further discussion is provided in the following.

Quality assurance tests

Quality assurance tests are performed during manufacturing to confirm compliance of the as-produced product with specifications.

**Guidance note:**

Quality assurance tests shall be used to verify the quality of supplied subsystems (components), when this is required to manage critical parameters in the Technology Qualification Process, e.g. material properties, dimensional accuracy, contamination level of hydraulic fluids, electrical resistance).

Factory acceptance tests

Factory acceptance tests (FAT) shall provide as much evidence as possible that the system, equipment or component is fit for purpose and performs according to its functional specification before it leaves the factory. The tests represent part of the Quality Control procedure. They shall provide confidence that gross manufacturing defects are not present. The items to be included in the tests shall be those identified in the Technology Qualification Process. Undertaking a FAT clearly delineates responsibility and reduces uncertainty.

**Guidance note:**

A factory acceptance test can be performed where practical in order to reduce damage probability or uncertainty in the qualified product.

Pre and post installation tests

Pre and post installation tests shall provide evidence that the performance of the as-delivered and installed technology conforms to Technology Qualification Basis. These tests represent a part of the Quality Control
procedure and provide confidence that gross assembly defects are not present. All the items identified in the Technology Qualification Process should be included over and above any such testing that would normally be undertaken for proven technology.

Pilot Application

Pilot applications are intended to increase the confidence in the reliability through documentation that all failure modes have been addressed appropriately in the prior qualification activities, as well as reducing the probability of undetected failure modes.

9.5 Documented Experience

Relevant experience data can be a valuable source of evidence when performance of components or functions shall be documented. Even if existing historical data is not directly applicable to novel technology, it can provide valuable input to the Technology Qualification Process:

— Historical data can be obtained and adjusted to fit the novel technology by evaluating the respective differences in effect of the critical parameters.
— Historical data may be available for sub-systems, functions, or individual components of the novel technology. This can be utilized when the novel technology is subdivided into manageable elements as part of the Technology Qualification Process, especially in cases where the novel technology consists of sub-systems, functions and components that are proven, but put together in a new and different way.

Hence, historical data can be either be directly applied to parts of the technology, or applied with some adjustment to take differences in configuration or application into account. App.E includes a more detailed discussion on this subject. See also guidance note in Sec.[8.5.1].

9.6 Methods to Document Uncertainty, Probability of Failure and Margins

The relevant sources of uncertainty for the qualification shall be documented.

Guidance note:

Uncertainties are typically related to the following parameters:

Robustness
- input parameters
- erroneous operation
- interfaces
- fluid flow and environment
- loads
- analysis
- tests
- fabrication tolerances
- transportation
- installation
- operation
- extreme limit
- combined, overall margins and reliability.

Margins towards typical failure modes
- material degradation
- exceeding tolerance limits
- electrical insulation degradation
- clogging
- leak
- rotor dynamics - failure
- strength static - failure
- strength dynamic - failure
- impact resistance - failure
- particle interactions - failure
- mechanisms - failure
- function failure
- power failure
- control and sensor failures.

Conventional engineering methods normally express safety margins as “safety factors” that account for the underlying uncertainties.
It is acceptable to adopt the margins specified in a validated set of requirements (such as an applicable standard, industry practice or specification), provided uncertainties accounted for by the margins be the same as those of the novel technology. This evaluation shall be documented as part of the validation of requirements.

If the uncertainties accounted for by the standard, industry practice or specification differ from those of the novel technology, the same margins shall not be used directly. It is then acceptable to substantiate that an equivalent safety level is achieved as the level implied by the relevant standard, industry practice or specification.

If no relevant standard, industry practice or specification is available, the probability of failure shall be determined based on best industry practice.

Guidance note:
There are four approaches to determining the probability of failure:

1) Engineering judgement.
2) Statistical evidence from testing or field experience.
3) Probabilities defined through application of standards.
4) Probabilities found by structural reliability methods (probabilistic method).

A probability based on engineering judgement will in some form be based on statistical evidence through experience. Personal qualifications are hence of importance as discussed in Sec. [4.4]. This implies that there is a significant uncertainty to the estimated probability, which shall be conservative.

Statistical evidence from testing or field experience can be handled based on ISO’s “Guide to the Expression of Uncertainty in Measurements”.

Structural reliability assessment can be carried out based on DNV Classification Note 30.6 or other established industry practice. The method is illustrated in Figure 9-1, where S is the probability density distribution of the load effect, and R is the probability density distribution of the resistance.

For failure mechanism material plastic yield, S is the probability density distribution of the stress in response to the applied load, and R is the probability density distribution of the yield stress. Failure occurs when S exceeds R as illustrated by the range where the distributions overlap with a non-negligible probability. Quantification of the probability uses the joint probability density distribution f_{R,S}.

![Figure 9-1](image)

The probability density distributions according to probabilistic design, indicating the range where the distributions overlap with a non-negligible probability density
10 Execution of the Technology Qualification Plan

Execution of the Technology Qualification Plan should document the performance margins for the failure modes of concern.

10.1 Introduction

The execution of the Technology Qualification Plan usually represents the main cost in the Technology Qualification process, and may be time consuming compared to the previous steps. It is therefore important that the qualification activities are well chosen and planned in order to derive the maximum value from the investment in time and resources, by generating the information needed to address the identified failure modes.

The execution of the Technology Qualification Plan consists of the following key steps:

— Carrying out the activities in the Technology Qualification Plan.
— Collecting and documenting the data generated by the respective qualification activities.
— Ensuring traceability of this data.
— Determining the performance margin for each failure mode.

Guidance note:

If there is a delay between the development of the Technology Qualification Plan and its execution, it is recommended that it should be reviewed to ensure that the qualification activities still properly address the failure modes of concern:

— Check/verify that the planned activity for each failure mode will address the performance margins of concern.
— Will the planned test find the performance margin to the specified operational requirements with the desired level of confidence?
— Check that the operational limits specified in the Technology Qualification Basis are correct for each failure mode of concern. Check with the Critical Parameters List.
— Verify that the planned tests will validate the analytical model(s).
— Verify the level of accuracy.
— Outline what is sufficient evidence and how evidence should be generated and documented.

The activities of the Technology Qualification Plan shall be executed as specified, unless the deviation is planned i.e. it stems from the iteration process.

The assumptions and conditions that need to be fulfilled by the qualified technology shall be documented.

10.2 Failure Mode Detection During Qualification

Failure modes detected during the quality control at manufacturing, qualification tests, fabrication acceptance tests or later operations shall be recorded and documented. The documentation shall include the date detected, the description of the failure mode, other observations and the identity of the originator.

When a failure or failure mode is detected in the Technology Qualification Process, the occurrence of the failure mode shall be evaluated with regard to the three following cases:

1) Failure mode occurred within the expected frequency of occurrence according to the analysis.
2) Failure mode occurred with a higher frequency of occurrence.
3) Failure mode has not been considered.

In case 1 no further action needs to be taken. In case 2 the basic assumptions for the frequency of occurrence shall be re-evaluated. This re-evaluation shall include implications for all models used. In case 3 the failure mode needs to be considered and if found relevant must be included in the Technology Qualification Process.

10.3 Collection and Documentation of Data

The documented evidence from the execution of the Technology Qualification Plan shall enable the performance assessment step to be carried out. The data collection and its documentation should be performed at the level of detail relevant for the development stage of the technology.

The quality of the data generated and compliance with the specification in the Technology Qualification Plan shall be evaluated.

The failure mode register (Sec.[8.1]) shall be used to follow up the data collection and the overall qualification of the technology.

Guidance note:

An electronic database may be used for this purpose when the technology has many parts, sub-systems or failure modes, i.e. in excess of 25. The purpose of this database is to:

Keep track of the qualification development for each failure mode and for each part sub-system.

An electronic database shall be arranged to allow for automatic sorting with the purpose to extract and present key data and issues in priority. This can include:
1) the failure mechanisms within the medium and high risk area
2) the failure mechanisms with shortest time to failure
3) the parts or sub-systems with shortest time to failure
4) parts subject to similar type failure mechanisms
5) common-mode failures
6) the failure mechanisms related to the risk categorization of the technology.

Appendix A illustrates a simple form of such an electronic database checklist based on a spread-sheet with database facilities. This allows for sorting based on information in any of the columns.

Each revision of the checklist shall be identified as well as the sources for input into the checklist.

---e-n-d---of---G-u-i-d-a-n-c-e---n-o-t-e---

In order to ensure traceability, the data shall be organized in such a manner that there is a clear link between the steps of the Technology Qualification Process, from the Technology Qualification basis to Performance Assessment. It shall be possible to trace the threats that have been identified, how they have been addressed (tests, analysis, previous experience, etc.), what evidence has been developed (test and analysis reports), and how that evidence meets requirements in the Technology Qualification Basis.

This provides opportunity for independent review of the qualification conclusions and will enable reuse of evidence in future projects, e.g. qualification of refined versions of the technology or other technology based on elements of this technology.
11 Performance Assessment

The objective of Performance Assessment is to measure success by reviewing the available qualification evidence (Sec.10) against the Technology Qualification Basis (Sec.6). In the final iteration, this implies confirmation that the technology meets all its requirements, and both risk and uncertainty have been reduced to acceptable levels. In earlier iterations, where health, safety or the environment shall not be compromised, a Performance Assessment can include a judgement that the risk and uncertainty relating to the remaining part of the Technology Qualification Plan is acceptable.

11.1 Introduction

The purpose of this Performance Assessment is to provide confidence and remove uncertainty from the links between the evidence, failure modes and the requirements in the Technology Qualification Basis. If the assessment concludes that some functional requirements of the technology are not met, risk control options (modification of the technology) and further qualification activities can be identified. This can include tightening of the operating envelope, or to enhance inspection, maintenance and repair strategies to meet the requirements based on the existing evidence. If none of these are feasible, the Technology Qualification has failed.

Performance Assessments can also be carried out at defined points during operation, to confirm that the operations are within the assumptions contained in the Technology Qualification Basis.

Key steps of the Performance Assessment are to:

— Interpret the evidence in the specific context of the technology, to account for simplifications and assumptions made when the evidence was generated, and limitations and approximations in the methods used.
— Confirm that the qualification activities have been carried out, and that the acceptance criteria have been met. A key part of this confirmation is to carry out a gap analysis to ensure that the qualification evidence for each identified failure mode (Sec.8) meets the acceptance criteria.
— Perform a sensitivity analysis of relevant parameter effects.
— Assess the confidence that has been built into the qualification evidence through the qualification activities. This shall consider the extent to which test specifications have been independently reviewed, and tests witnessed by an independent party.
— Compare the failure probability or performance margin for each identified failure mode of concern with the requirements laid down in the Technology Qualification Basis. Evidence shall be propagated for individual elements of novel technology and reviewed against the entire system covered by the Technology Qualification.

When parameter effects are predicted by models, the assessment must include validation of the models used.

When service records are used in the assessment, the conditions in which the recordings were made shall be accounted for; and the assessment shall consider how the intended service conditions differ.

When evidence from component or prototype tests is used, the assessment shall account for the actual tolerances achieved in the objects tested, relative to the tolerances specified for the technology; thereby accounting for any deviations between the performance of the test objects and those already in production.

The qualification conclusions might represent a safe service envelope (that would permit safe operation at an acceptable level of risk) beyond the operating conditions specified in the Technology Qualification Basis. This can simplify re-qualification for modified operating criteria, i.e. a wider service context.

11.2 Reliability

11.2.1 General

If a reliability target is stated in the Technology Qualification Basis, then a quantitative reliability assessment shall be carried out, taking into account information from the execution of the Technology Qualification Plan.

For time-dependent failures, the estimated time to failure shall be referred to a specified time reference, e.g. the overall (total) system lifetime or planned time to maintenance.

The overall failure probability of a system is governed by:

— the failure modes of the individual components in the system
— the probability of these failure modes
— the lifetime probability density distribution, which is a function of time, special operations or other parameters
— any dependencies between components or common causes that may lead to multiple failure modes
— the consequence of failure modes on the system failure frequency taking into account redundancy.

Several established methods can be used to estimate reliability. They are briefly described in the following.
11.2.2 Input data

The reliability analysis shall be based on the failure modes established according to Sec.8. The reliability analysis shall be based on the evidence gathered during execution of the Technology Qualification Process.

11.2.3 Methods

Common methods for estimation of the system reliability are:

— Reliability block diagram technique (RBD), which considers system with components in series and parallel.

— Fault tree analysis (FTA), which considers combinations of subsystems, lower-level faults and component faults. FTA is a top-down analysis, and therefore has to be repeated for each top event.

— Monte Carlo simulation of RBDs, FTs or more complex systems utilizing some suitable software tool.

The standard found best to describe these systems is: BS 5760: Part 2 (1994), Reliability of systems, equipment and components, Part 2. Guide to assessment of reliability.

ISO 20815 describes the modelling of production systems.

Guidance note:
A reliability goal might be 90% probability of no total function failure within the specified time.
Many failure mechanisms are related to time and operations. They have an increasing probability of occurrence with service life. In the analysis, this effect is described by the probability distribution. Hence it is of particular importance to establish a distribution for the failure with highest risk.

Failures occurring in the early phases of operation are often related to manufacture or installation. A high quality of pre-installation checks and tests upon installation will reduce such risk. Therefore the analysis should include a focus on the effects of such checks and tests, as well as quality management practices to prevent faults from occurring in the first place.

For a complex system, the system reliability and its associated distribution may be determined by simulation techniques.

A complex system has many failure modes, each with its associated failure probability distribution. The system reliability and its associated distribution may be determined by Monte Carlo simulation techniques. The system reliability is calculated a large number of times. For each calculation a new failure probability is determined for each failure mode drawn from the statistical distribution of that particular failure mode. The resulting system reliability values add up to form a failure probability distribution for the overall system. The system mean time to failure and other statistical parameters, such as lower acceptance quantile, say, 90% probability of no failure, may be calculated based on this distribution.

There is a range of computer programs on the market for this purpose.

When relevant reliability data are lacking, structural reliability assessment (SRA) methods can be used to estimate the reliability of novel structural elements and components. SRA is based on models of the failure mechanisms. Some general principles are provided in ISO 2394: General Principles on Reliability for Structures, whereas more practical guidance is provided by DNV Classification Note 30.6: Structural Reliability Analysis of Marine Structures. These methods can be used whenever a failure mode can be represented as a limit state function (model) formulated in terms of random variables that represent the relevant sources of uncertainty.

11.3 Decision-making

The Performance Assessment concludes with the appointed decision-maker concluding whether or not a specific milestone (qualification state) in the Technology Qualification Programme has been reached.

In general, the decision-making is based on:

— Demonstration of compliance with the requirements specified in the Technology Qualification Basis.

— Judgement - presented by experts or an independent party – whether or not the specified development stage has been reached.

— The confidence that the decision-makers have acquired through their better understanding of the novel technology.

This positive or negative outcome constitutes the deliverable of Technology Qualification as described in this Recommended Practice, and is the only measure of the confidence that has been established in the technology.
APPENDIX A  CHECKLIST - FAILURE MECHANISMS - DATA BASE

A.1  Failure mechanisms checklist

Table A-1 represents a table layout combining data needed to follow up failure mechanisms as well as general FMEA – FMECA data. It is practical to arrange this in a database to enable automatic sorting and follow up the failure modes of concern, failure mechanisms, and items of new technology. The FMEA – FMECA data are normally of interest in the early development phases, when risk is associated with categories for probability and consequence.

The left part of the table relates to the reliability data collection, when focus is on documenting lifetime for the failure mechanisms. The desirable degree of completeness when filling out the table depends on the later use and the expected results from automatic sorting. New lines need to be inserted in the table during the development and qualification. The practical identification of the lines will therefore be the part number and failure mechanism type. The ID number only follows the sequence of inserts, unless it is decided to use a sequential number linked only to the part number and failure mode.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identification number</td>
</tr>
<tr>
<td>Failure Mechanism Type/Root cause</td>
<td>See RP</td>
</tr>
<tr>
<td>Part No</td>
<td>The part number(s) identifying the parts on an arrangement drawing (position numbers) or subsystem identification on a schematic system arrangement</td>
</tr>
<tr>
<td>Risk Cat.</td>
<td>Risk Category:</td>
</tr>
<tr>
<td></td>
<td>— L = Low</td>
</tr>
<tr>
<td></td>
<td>— M = Medium or</td>
</tr>
<tr>
<td></td>
<td>— H = High</td>
</tr>
<tr>
<td></td>
<td>Automatically calculated based on the frequency and consequence category at the end of the table.</td>
</tr>
<tr>
<td>Novelty Category</td>
<td>Novelty category for the technology: Ranging from 1 to 4 according to the Sec.[7.3].</td>
</tr>
<tr>
<td>MTTF</td>
<td>Mean Time To Failure. The average time to failure, e.g. expectancy of a probability distribution, is a useful parameter from the probability distribution.</td>
</tr>
<tr>
<td>LCL</td>
<td>Lifetime at the acceptable confidence level defined by the acceptance percentile, Fig.3-1. E.g. the lifetime at a confidence level, e.g. 95%, will change during the qualification as the lifetime probability density distribution is improved.</td>
</tr>
<tr>
<td>Margin</td>
<td>Margin between operating condition and failure condition as determined in the reliability data collection. This is in particular relevant for failure mechanisms which are not due to degradation and for which “Failure Rate” becomes irrelevant.</td>
</tr>
<tr>
<td>Comment</td>
<td>Comments needed to understand the information given.</td>
</tr>
<tr>
<td>Source</td>
<td>The source for Failure rates and Margin determination (document reference), as well as identification of the person making the last revision.</td>
</tr>
<tr>
<td>Rev</td>
<td>Last revision number for the particular failure mechanism.</td>
</tr>
<tr>
<td>Date</td>
<td>Date of last revision.</td>
</tr>
<tr>
<td>Failure Mode</td>
<td>Identification of the failure mode</td>
</tr>
<tr>
<td>Detection</td>
<td>Possible method assumed for detection of the failure mode</td>
</tr>
<tr>
<td>Effect</td>
<td>The effect on the overall system.</td>
</tr>
<tr>
<td>Operating phase</td>
<td>The operational phase for which the failure mode is assessed.</td>
</tr>
<tr>
<td>Service life</td>
<td>Target service life for component/function.</td>
</tr>
<tr>
<td>Revised Frequency category</td>
<td>An updated failure probability category defined according to the risk matrix. Input information is from MTTF or LCL.</td>
</tr>
<tr>
<td>Revised Cons. category</td>
<td>An updated consequence category according to the risk matrix.</td>
</tr>
<tr>
<td>Initial Frequency category</td>
<td>The initial failure probability category. This is part of the quality control to track changes. A check to ensure that the failure mode is considered after changes/modification.</td>
</tr>
<tr>
<td>Initial Cons. category</td>
<td>The initial consequence category. Ref. above.</td>
</tr>
<tr>
<td>ID</td>
<td>Failure mechanism type / Root cause</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX B  ITEMS OF CONCERN – CAUSES OF FAILURE MECHANISMS – TECHNOLOGY DEVELOPMENT STAGE

B.1 Introduction
Listed in this appendix are checklists to be used as guidance to different sections of this Recommended Practice. They are meant to help the Technology Qualification Process either by simple or leading questions, or defined issues that can easily be overlooked in a complex technology. The lists are meant as examples and are therefore not complete. The headings of the following main sections reflect the related headings in the main part of the Recommended Practice.

B.2 Technology Qualification Basis

B.2.1 System description
The following is related to specifications of systems/components:

System description
Capacities (Capacity requirements and limit conditions shall be clearly stated in the system specification)
Certificates, approval
Component lists
Connections/Interface
Delivery (Scope)
Dimensions
Environmental data of operation
Failure rate, lifetime, availability
Function description
I/O signals
Installation
Instrumentation
Layout, drawings
Maintenance
Mounting
Operation
Operation manual
Operation limits
PID documentation
Purpose of the system
Safety systems
Standards, rules and regulations
System specifications
Vendor interfaces

B.2.2 Uncertainties
The following checklist summarises items that should be considered continuously throughout the design process with regards to inherent uncertainties.

Analysis
Dynamic responses
Input parameters
Installation
Interfaces
Vendor deliveries
Loads
Sea bed
Tests
Time (to completion, lifetime, for operation)
B.3 Ranking of Failure Modes

The failure causes have been grouped in categories, like type of equipment etc.

B.3.1 Failure causes

Materials
Brittle fracture
Cathodic protection
Corrosion
Erosion
Explosive decompression
Fatigue
H₂S internal and external
Material compatibility
Material degradation and ageing (Metallic materials, polymers, and composites
Mechanical properties and temperature
Migration in thermal insulation and buoyancy materials
Swelling

Mechanical equipment
Balance
Bearings
Cavitation
Impact
Mating/inter facing
Migration causing leak
Operation
Thermal expansion
Vibration
Water lock
Wear

Electrical Power systems
Ageing
Connectors (mating, malfunction)
Electrical insulation degradation
High voltage
Low voltage
Migration
Transmission losses

Optical systems
Cable break
Cable loss
Connectors losses
Electro-optical equipment malfunction

Pneumatic systems
Clogging
Contamination and condensation
Control system loss
Pressure loss
B.3.2 Functional elements

Rotor dynamics
Seals
  — Static soft seals
  — Dynamic soft seals
  — Static hard seals
  — Dynamic hard seals
  — Dynamic fluid seals
Soil interactions
Strength dynamic
Strength static

B.3.3 Interfacing power and control system failure

Electric power
Electronic control and sensor failures
Hydraulic
Manual
Software

B.4 Technology Development States and Readiness Levels

Industry uses Technology Readiness Levels (TRL) as a measure of a technology's qualification development state. The Technology Readiness Level can be defined both for a system and for components. The scale varies from rough ideas to field proven technology, and the level is normally determined by the amount or scale of performed tests.

Various scales and descriptions are in use by the industry today. It should be verified that the scale to be used defines relevant readiness levels for the technology being qualified.

The generic TRL definitions used in industry can be aligned with the technology qualification states, ref. Figure 4-2. Because the acceptance criteria are ambiguous, it is difficult to determine when each TRL has been reached. If it is required in the Technology Qualification Programme to identify TRLs, then project specific acceptance criteria should be developed for each relevant TRL.

TRLs provide a high-level measure of the progress of the technology development, and the associated qualification state, suitable for comparing similar technologies.

When Technology Readiness Level is used in conjunction with qualification of technology to communicate the...
qualification state, it shall be verifiable through evidence from qualification activities according to this Recommended Practice.

Experience has shown that high focus on TRL assessments can require a lot of time and resources and does not contribute to enhancing the technology.

For this reason it is recommended to complement the use of TRLs with other ways of assessing qualification status. That can be progress towards specified milestones, project risk assessment concerning schedule and budget risks, and assessment the risk of failing to achieve qualification.

Table B-1 shows the TRLs defined in by US DoD Technology Readiness Assessment (TRA) Deskbook (July 2009). They are supported by detailed guidance in the Deskbook on the use of the TRLs that is relevant for the intended military application areas. Table B-2 below shows the TRLs defined in API 17N, Recommended Practice for Subsea Production System Reliability and Technical Risk Management (2009). Detailed guidance similar to that in the DoD Deskbook is not available for subsea systems. These tables are shown for information purpose only.

**Table B-1  TRLs defined by US DoD**

<table>
<thead>
<tr>
<th>TRL</th>
<th>US DoD Deskbook Description for hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>[Not used]</td>
</tr>
<tr>
<td>1</td>
<td>Basic principles observed and reported</td>
</tr>
<tr>
<td>2</td>
<td>Technology concept and/or application formulated</td>
</tr>
<tr>
<td>3</td>
<td>Analytical and experimental critical function and/or characteristic proof of concept.</td>
</tr>
<tr>
<td>4</td>
<td>Component and/or breadboard validation in a laboratory environment</td>
</tr>
<tr>
<td>5</td>
<td>Component and/or breadboard validation in a relevant environment</td>
</tr>
<tr>
<td>6</td>
<td>System/subsystem model or prototype demonstration in a relevant environment</td>
</tr>
<tr>
<td>7</td>
<td>System prototype demonstration in an operational environment</td>
</tr>
<tr>
<td>8</td>
<td>Actual system completed and qualified through test and demonstration</td>
</tr>
<tr>
<td>9</td>
<td>Actual system proven through successful mission operations</td>
</tr>
</tbody>
</table>

Lowest level of technology readiness. Scientific research begins to be translated into applied research and development (R&D). Examples might include paper studies of a technology’s basic properties.

Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative, and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.

Active R&D is initiated. This includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.

Basic technological components are integrated to establish that they will work together. This is relatively “low fidelity” compared with the eventual system. Examples include integration of “ad hoc” hardware in the laboratory.

Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so they can be tested in a simulated environment. Examples include “high-fidelity” laboratory integration of components.

Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology’s demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.

Prototype near or at planned operational system. Represents a major step up from TRL 6 by requiring demonstration of an actual system prototype in an operational environment (e.g., in an aircraft, in a vehicle, or in space).

Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation (DT&E) of the system in its intended weapon system to determine if it meets design specifications.

Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation (OT&E). Examples include using the system under operational mission conditions.
<table>
<thead>
<tr>
<th>TRL</th>
<th>API 17N</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td><strong>Unproven Concept</strong>&lt;br&gt;Basic R&amp;D, paper concept</td>
</tr>
<tr>
<td>1</td>
<td><strong>Proven Concept</strong>&lt;br&gt;Proof of concept as a paper study or R&amp;D experiments</td>
</tr>
<tr>
<td>2</td>
<td><strong>Validated Concept</strong>&lt;br&gt;Experimental proof of concept using physical model tests</td>
</tr>
<tr>
<td>3</td>
<td><strong>Prototype Tested</strong>&lt;br&gt;System function, performance and reliability tested</td>
</tr>
<tr>
<td>4</td>
<td><strong>Environment Tested</strong>&lt;br&gt;Pre-production system environment tested</td>
</tr>
<tr>
<td>5</td>
<td><strong>System Tested</strong>&lt;br&gt;Production system interface tested</td>
</tr>
<tr>
<td>6</td>
<td><strong>System Installed</strong>&lt;br&gt;Production system installed and tested</td>
</tr>
<tr>
<td>7</td>
<td><strong>Field Proven</strong>&lt;br&gt;Production system field proven</td>
</tr>
</tbody>
</table>
APPENDIX C  EXAMPLES OF APPLICATION

C.1 Introduction
This appendix includes examples of the application of the methods described in this Recommended Practice for real equipment as an extended guidance:

— a subsea booster pump, Framo (installed on Lufeng)
— qualification of a component to be mass-produced and used in different systems
— a subsea multiphase pump; Kværner Eureka (demonstrator for the development project).

C.2 A Subsea Booster Pump, Framo

C.2.1 Introduction

C.2.1.1 Example
This example pump is similar to a pump, which has been in operation since January 1998 in 330m water depth in the South China Sea, on the field termed “Lufeng”. The pump has been designed and manufactured by Framo Engineering AS.

C.2.1.2 Applied data
The technical data used in this example is based on information generally available on the Internet. The available real data is therefore limited. When supplementary data is needed for illustration, the data is based on assumptions and best guesses. Hence, this example is not related to the actual case.

C.2.1.3 The example set in the development time frame
The example is assumed to have passed a concept phase and is into the development and engineering phase. Throughout the example, different steps in this phase have focused on how to give the best examples when using this Recommended Practice.

C.2.2 Technology Qualification Basis (Sec.6)

C.2.2.1 General
For a general arrangement of the pump see Figure C-3. The pump consists of approximately 100 items and 500 parts (e.g. including number of bolts).

C.2.2.2 Contents of the specification
The data and documentation listed in Table C-1 must be made available for the Technology Qualification Process, and as the specification of the subsea booster pump, qualified according to the Recommended Practice.

Table C-1  A table of typical required data for the different phases of operation

<table>
<thead>
<tr>
<th>Booster pump main technical data:</th>
<th>Drawings Method of operation</th>
<th>Flow rate: 130 m³/h</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facts:</td>
<td></td>
<td>Maximum pressure: 228 bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pressure gradient: 35 bar</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max depth: 330 m</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Service life: 7 years</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating temperature: 4°C</td>
</tr>
<tr>
<td>Medium:</td>
<td></td>
<td>Gas, oil, water mixture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pH level: 5-9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max GOR: 7%</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max H₂S: 5 ppm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max CO₂: ZZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max particle size: XX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Max particle rate: YY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Separate installation</th>
<th>Method</th>
<th>Maximum loads:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maximum wave heights:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum sea currents:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum landing speed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tool and vessel requirements</td>
</tr>
</tbody>
</table>
Table C-1 A table of typical required data for the different phases of operation (Continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Booster pump main technical data:</th>
<th>Drawings Method of operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation</td>
<td>Start</td>
<td>Loads</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valve status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flow conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power consumption</td>
</tr>
<tr>
<td>Stop (planned)</td>
<td>Loads</td>
<td>Power need</td>
</tr>
<tr>
<td>Shut-in operation</td>
<td>Medium data</td>
<td>Power</td>
</tr>
<tr>
<td></td>
<td>Shut-in shock</td>
<td>Flow properties</td>
</tr>
<tr>
<td>Emergency shutdown</td>
<td>Power</td>
<td>Flow properties</td>
</tr>
<tr>
<td>Variation of load</td>
<td>Flow data</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Power</td>
<td></td>
</tr>
</tbody>
</table>

Table C-2 A list of technologies and environments

<table>
<thead>
<tr>
<th>Item</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Subsea operations (330 m depth, installations and retrieval)</td>
</tr>
<tr>
<td>2</td>
<td>Pump design</td>
</tr>
<tr>
<td>3</td>
<td>Multi phase flow</td>
</tr>
<tr>
<td>4</td>
<td>Electrically powered (from topsides unit, high voltage and electrical motor design)</td>
</tr>
<tr>
<td>5</td>
<td>Control and Condition monitoring</td>
</tr>
</tbody>
</table>

C.2.2.3 Critical parameters list

The dimensioning loads and operational parameters are to be included in a list to be used to check that these have been considered and addressed in the qualification tests, and that any change to these parameters is reflected in the qualification activities.

C.2.2.4 Qualification team

Table C-3 The following team is assigned to establish the failure modes and failure mechanism. (See CV’s (not enclosed))

<table>
<thead>
<tr>
<th>Personnel</th>
<th>Subject</th>
<th>Items</th>
<th>Years experience/ Education</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mrs. Larsen</td>
<td>Subsea engineer</td>
<td>1</td>
<td>12, Engineer</td>
</tr>
<tr>
<td>Mr. Olsen</td>
<td>Process engineer</td>
<td>3</td>
<td>8, M.Sc</td>
</tr>
<tr>
<td>Mrs. Hansen</td>
<td>Electrical power systems</td>
<td>4</td>
<td>10, Dr.Ing</td>
</tr>
<tr>
<td>Mr. Pedersen</td>
<td>Maintenance and condition monitoring</td>
<td>5</td>
<td>6, B.Sc</td>
</tr>
<tr>
<td>Mrs. Halvorsen</td>
<td>Materials engineer</td>
<td>2</td>
<td>15 Metallurgist</td>
</tr>
</tbody>
</table>

C.2.3 Technology Assessment (Sec.7)

The Recommended Practice proposes two ways of subdividing the system; based on functions or based on hardware components. Both the proposed methods are shown below. The benefit of the functional approach is that early in the overall process one identifies failure modes on a functional level.

The subsea multiphase pump is composed of items normally found in hydrocarbon-processing pumps in general. The technology novelty category is 3 due to the following: The pump type is recently put in use in a novel application area (subsea).

The “novel” and critical features are:

— High reliability is required. Thereby standard components require special considerations.
— Some areas (sub-assemblies) of the pump design are not standard issue.
— The maintenance philosophy is not standard (as for a topside application).
— The pumped fluid is not conventional, and may change over time.

Most of the items of the pumps are proven in typical environments. But the high reliability requirement in subsea applications, however, leads to the definition of the items and sub-assemblies into two categories:

a) Items with no deteriorating mechanisms provided they are protected against corrosion and have sufficient strength.

b) Items with an operating life governed by wear, fatigue, erosion, changing of properties and other deteriorating mechanisms.

For Category a) the design standard and limiting conditions shall be addressed.

Category b) requires particular attention due to the high reliability requirement, and is therefore considered as “novel technology” in the following.

These category items as well as assemblies and performances shall be followed up by a “Quality plan”.

Examples:

The enclosure for the electrical motor:

Its purpose is to maintain a pressure barrier, transfer forces from installation tool, internal parts and induction forces, protect, and transfer heat. Further it shall keep the internal parts in position, including when deflected.

These are items, which can be addressed in the quality plan and followed up according to standard used procedures. Thereby the limiting condition can be established by aid of generally recognised standards and margin to a limit that can be verified.

The main dimensioning and material selection is thereby governed by a pressure vessel or structural standard with additions from a corrosion protection standard (galvanic corrosion and hydrogen embrittlement by cathodic protection) and related assumptions. The reliability of this item can be given the best rating, category 1. The following up of the “quality plan” represents the uncertainty area for this component.

Bolts

Bolts used for connecting the main components can be subject to the same procedure as above. In addition the required pretension needs to be justified and addressed in the quality plan.

Based on the above screening and the items found critical in regard to reliable service during their service life cycle, the items to be considered more thoroughly for qualification are:

a) Items subject to abrasive wear: dynamic seals, bearings, mating surfaces.

b) Items affected by impact loads during installation.

c) Items subject to erosion: impeller, stator.

d) Items subject to fatigue: ball and roller bearings, shaft.

e) Items subject to material property changes as function of time and environment: polymer seals, electrical insulation

f) Items subject to leak: mechanic seal system, polymer seal systems, responses to conditions caused by expansions, tolerances, temperature, pressure, fluids, time.

Further, effects from the system response on each item and the system responses themselves to be qualified:

a) Pump capacity as function of fluid type.

b) Most extreme fluid conditions causing impacts, erosion, cavitation, corrosion.

c) Motor and pump temperature as function of normal and extreme operating conditions.

d) Wear rate of seals and bearing as function of lubrication normal and extreme quality.

e) Leak rate of seals due to vibrations and wear.

f) Corrosive protection system including possible electromagnetic effects from the power.

g) Electrical power extreme conditions.

h) Shaft unbalance and straightness.

i) Installation and replacement conditions considering marine growth, water blocking, clearance tolerances, current and wave conditions.

j) Protection from likely sizes of dropped and dragged objects.

k) Likely operational failures.

l) Likely sensor and monitoring failures.

Component and unit system method (Sec.7.2.2)

For relatively limited systems, as this pump, it may be practical to initially consider the individual components and their failure modes. A disadvantage of this approach can be that combined and overall failure modes may be overlooked until late in the design process.
This method can be based on the item list from the general arrangement drawing of the pump motor assembly and a list of possible conditions and higher level and system failure modes that can have a negative effect on the items.

The first step is to divide the system into the subdivisions, e.g.:

- pump unit
- motor
- lubrication system
- power transmissions.

Each subdivision is divided into sub-components, ‘items’, e.g. impeller, shaft, bearings, seals, and Casing etc.

Each component has its failure modes, which is shown in Table C-4. Each failure mode has several root causes or failure mechanism types as is further illustrated in the same table.

Functional system analysis (Sec.7.3.2)

The objective of the following is to identify failure modes through sub-sectioning the system into functions and sub-functions until the function depends on a component.

The pumps main function can be divided in three:

- transport and installation
- operation
- abandonment.

The three functions are further sub divided (not extensive) according to Table C-4.

<table>
<thead>
<tr>
<th>Function</th>
<th>Subfunction</th>
<th>Subfunction/ Component</th>
<th>Subfunction/ Component/ Failure mode/Root cause</th>
<th>Component/Failure mode/Root cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport and installation 1</td>
<td>Sealing 1.1</td>
<td>Seal external 1.1.1</td>
<td>Leaking medium to external 1.1.1: F I</td>
<td>Scratch in sealing surface</td>
</tr>
<tr>
<td></td>
<td>Guide 1.2</td>
<td>Mateing 1.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Locking 1.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation 2</td>
<td>Pump medium 2.1</td>
<td>Pressurise medium 2.1.1</td>
<td>No differential pressurisation or reduced differential pressurisation 2.1.1: F I</td>
<td>Broken impeller(s) 2.1.1: F I a)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fracture fatigue</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Unbalance 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Pressure surge 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Fracture collision 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rotate impeller 2.1.2</td>
<td>Lubricate bearing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cool bearing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Motor operate</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Consume power</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Transfere torque from motor to impeller</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Structural integrity</td>
<td></td>
</tr>
<tr>
<td>Seal medium 2.2</td>
<td>Internal seal 2.2.1</td>
<td>Seal between stages</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Seal motor</td>
<td></td>
</tr>
<tr>
<td></td>
<td>External seal 2.2.3</td>
<td>Well medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Seawater inn</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Cooling medium out</td>
<td></td>
</tr>
</tbody>
</table>

Abandonment
C.2.4 Threat assessment (Sec.8)

The ranking of failure modes is a process in steps. Updates must be carried out for all steps in the overall process. In the first step all failure modes are identified and their criticality is assessed based on as is, without taking into account any mitigating measures, except normal engineering judgements for standard technology.

Criticality assessment of the failure mode “2.1.1: F I” is shown in Table C-5.

<table>
<thead>
<tr>
<th>Failure mode</th>
<th>Cause</th>
<th>Root cause</th>
<th>Consequence*)</th>
<th>Probability*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No pressurisation</td>
<td>Broken impeller</td>
<td>Fracture fatigue</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>2.1.1: F I a)</td>
<td></td>
<td>Unbalance 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fracture fatigue</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pressure surge 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fracture collision</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>2.1.1: F I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* The consequence and probability are ranged from 1 to 5 with 5 being the most severe consequence and the highest probability (see Sec.[7.4] or Table 7-1). These high probabilities are related to this example being in the development phase and to assure that they are given attention. It is anticipated that the high levels of consequence and probability will reduce as the qualification process proceeds.

The failure modes identified as medium and high risk are considered in the Technology Qualification Plan.

C.2.5 Technology Qualification Plan (Sec.9)

The following overall plan is identified for the qualification.

A Technology Qualification Plan is developed based on experiences, numerical analysis and tests, concentrating most efforts on the main items identified in the process, C.2.5.
The main principles of the plan are e.g.:

— To qualify each failure mode separately. Numerical analysis and the quality plan can qualify most of them. Thereby accelerated tests of the pump assembly will not be used to simulate the lifetime.
— To perform extended factory acceptance tests which include performance measurements as well as measurements of parameters that can cause deterioration of items. The latter can in submerged performance tests include lubrication temperature, leak measurements, leak response on shaft vibrations.
— Performance test of the pump with various gas-to-oil ratios and varying of the critical parameters.
— Installation test.

Cost reduction

It is assumed that the main uncertainties are related to some items and failure mechanisms, e.g., electrical coupling insulation resistance in salt water, impeller wear by sand production and pump performances at high gas oil ratios and slugging. The cost of possible uncertainty reduction, by further detailed qualification should therefore be evaluated.

Inaccuracies and uncertainties

Each numerical analysis and test, which includes measurements of parameters, shall include an estimate of the magnitude of inaccuracies.

Test

The above indicates the need for all types of tests including, basic tests, prototype tests and factory acceptance tests. The Technology Qualification Process must be concluded before final tests verifying the actual installation, and possible pilot application, which is represented by the earlier mentioned installation.

C.2.6 Execution of the Technology Qualification Plan (Sec.10)

Parameter effects

The critical parameters list was revisited to ensure that all parameters governing the critical failure modes are included. The following approach was used:

![Flowchart](image)

Figure C-2

A flowchart showing an approach to identifying parameters that are critical for a failure mode
Many components with a service life limit are selected according to sub-supplier’s qualified methods, for specified conditions. The quality of such selection methods varies from type of items and the sub-supplier.

**Example:**

**Bearings**  The pump selected as an example has a sliding thrust bearing based on tilted pads. The lubrication quality, running conditions and frequency of start and stop govern its lifetime.

The life of ball and roller bearings can be determined based on formulas given by the sub-supplier, which includes: rpm, number of cycles, type of bearing, constant for dynamic and static load sensitivity, alignment, temperature, lubrication quality. Hence, the main parameter dependencies can be established.

**Seals** Seal suppliers give selection criteria, but seldom formulas for life estimation. Therefore this requires effort in assessment. Without formulas, it is possible to establish important parameters based on the selection criteria and engineering judgement. Thus, uncertainties are larger than for the bearings.

**Impeller wear** Material loss rates can be based on developed formulas and experience, where such are available.

**Pump performance** Literature and experience establish formulas for pump performance. Multiphase requires particular experience, and formulas.

**Margin — Standard technology**

Established standards specify design acceptance criteria, which include safety margins against common uncertainties in materials and loads, e.g. for the enclosure for the electrical motor. Following up a margin to these criteria throughout the Technology Qualification Process therefore assures that the item remains with a probability of failure defined by the standard, i.e. one may be justified to use probability class 1.

**Margin — Technology that requires qualification**

Example: Thrust bearing- Failure type: Wear for sliding bearings (For a possible roller bearing: fatigue caused by rotation at load)

App.[C.2.4] defines novel technology for this example, and why the thrust bearing is put in this category. The thrust bearing is of a sliding type.

If a roller or ball bearing type had been selected, the size can be found in the bearing manufacturer’s manual, which normally will comply with ISO 282:1990. Such a manual can state that the dynamic load and rotation capacity of the bearing is specified as the 90% confidence interval, i.e. that 90% of a large number of bearings survive. Further it can state that 50% of the bearings experience approximately 5 times this specified rotational life.

Assuming that the failures follow a “Standard statistical distribution”, then the acceptance percentile as well as the mean time to failure (MTTF) can be established for the roller bearing for the intended operational life. A specific “margin” is therefore not relevant in this context. The margin is implicit given in the percentile and MTTF.

**C.2.7 Performance Assessment (Sec.11)**

Assuming that each separate failure mode will cause the pump to stop or malfunction, then the pump reliability can be described by the sum of each of the probabilities for the failure modes, i.e. by the “generic part method”. Both the sum of “mean time to failure” and the “lower confidence interval” should be calculated.

The assumption above will be conservative and to some extent misleading. It is more appropriate to distinguish and deal separately with:

— reliability related to failures caused by installation
— failures that will not cause lost or reduced pump performance
— reliability of pump unit based only on failure modes causing lost or reduced performance.

It is assumed that the field life is 5 years. A reasonable “lower confidence level” for the pump is assumed to be 10%, i.e. that the pump performs as intended is estimated with 90% reliability within this time period (one out of 10 failures within the period).

Assuming further that only the 10 most likely item and failure modes contribute to this reliability, and that the contribution from the rest of the items are calculated to be insignificant. The reliability estimate consequently should also be used as a loop in the early phase of the Technology Qualification Process. This will facilitate a concentration on the most important items, those with least reliability and with most uncertainties.
Figure C-3
A cross section of the pump
### Table C-6 Tabulated information, FMECA and checklists

<table>
<thead>
<tr>
<th>ID</th>
<th>Failure mechanism type / Root cause</th>
<th>Part No:</th>
<th>Risk Cat.</th>
<th>Tech Cat.</th>
<th>MTTF</th>
<th>LCL</th>
<th>Margin</th>
<th>Comment</th>
<th>Source</th>
<th>Rev</th>
<th>Date</th>
<th>Failure Mode</th>
<th>Detection</th>
<th>Effect</th>
<th>Revised Frequency category</th>
<th>Revised Cons. category</th>
<th>Initial Frequency category</th>
<th>Initial Cons. category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>Material fatigue, unbalanced cased.</td>
<td>Impeller</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>2 5 2 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Material fatigue, fluid cased.</td>
<td>Impeller</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>1 5 1 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Brittle fracture, Unidentified body</td>
<td>Impeller</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Brittle fracture</td>
<td>No pumping pressure</td>
<td>1 5 1 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Erosion/corrosion</td>
<td>Impeller</td>
<td>M 2</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Material loss</td>
<td>Reduced pump pressure</td>
<td>4 2 4 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>System failure, Clogging</td>
<td>Impeller</td>
<td>L 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Blocking</td>
<td>Reduced pump pressure</td>
<td>1 2 1 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Installation damage</td>
<td>Seal Pumpfluid - sea</td>
<td>M 2</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of pump fluid to sea</td>
<td>2 4 2 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Extrusion</td>
<td>Seal Pumpfluid - sea</td>
<td>M 3</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of pump fluid to sea</td>
<td>2 4 2 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>Ageing</td>
<td>Seal Pumpfluid - sea</td>
<td>L 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of pump fluid to sea</td>
<td>1 4 1 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Wear</td>
<td>Dynamical seal</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of lubrication into pump fluid</td>
<td>4 3 4 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Vibration</td>
<td>Dynamical seal</td>
<td>M 2</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of lubrication into pump fluid</td>
<td>3 3 3 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Leak</td>
<td>Dynamical seal</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Leak</td>
<td>Leak of lubrication into pump fluid</td>
<td>2 3 2 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1</td>
<td>Fatigue, rotational load</td>
<td>Trust Bearing</td>
<td>M 2</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>2 5 2 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.2</td>
<td>Overload, static</td>
<td>Trust Bearing</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>2 5 2 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.3</td>
<td>Wear, Loss/ contamination of lubrication</td>
<td>Trust Bearing</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>2 5 2 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.4</td>
<td>Wear, High lubrication temperature</td>
<td>Trust Bearing</td>
<td>M 1</td>
<td>BeMo 1</td>
<td>25.08.00</td>
<td>Cracking</td>
<td>No pumping pressure</td>
<td>2 5 2 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Legend:  
H = High risk category (over 15)  
M = Medium risk category (between 4 and 15)  
L = Low risk category (under 4)
C.3 Qualification of Mass-produced Components

C.3.1 Introduction

Some new type components are mass produced and intended for service in several types of systems. The qualification of such a component requires a rational approach to cover a range of services, different load cases and environments.

The following is an outline of such a qualification approach.

C.3.2 The typical process of a component qualification

An example of component qualification includes:

1) Perform a component application review: Identification of all loads, constraints and conditions that may have an impact on the component during its service life.
2) Establish a qualification tactic: Identify the best approach for a thorough qualification.
3) Carry out a component categorization: Based on the application review and assessments of future needs, categorize the component into standard application classes, for example pressure, size, fluids.
4) Define a qualification plan.
5) Execute the qualification tests.
6) Generate a qualification report.

Items 1 to 6 above comprise the Technology Qualification Plan (Sec.9).

C.3.3 Overall planning through developing procedures

The development and qualification of components is an iterative process involving all stages from specification to acceptance. Procedures to apply during the Technology Qualification Process must therefore be developed.

C.3.4 Requirement to documentation

The qualification procedures and reports shall include the component categorization data. Especially important is to highlight any changes to the categorization as resulting from the tests. Before a component is approved for use, all the qualification reports shall be reviewed and approved. The requirements for qualification testing given herein apply both to company components and to sub-vendor's components. The requirements shall be considered for each component and exceptions highlighted using the qualification notification system.

C.3.5 Accelerated testing

Since component expected service life is normally long, accelerated life testing is required. Some guidelines related to accelerated life testing shall be developed, but it must be emphasised that the engineer responsible for the qualification testing must review these on a case-to-case basis. Exceptions shall, however, be documented in the qualification test procedure and report.

C.3.6 Full-scale testing

It is difficult to predict all operational constraints and conditions of a component due to a variety of applications, and since some systems are complex and as such have not yet been planned or designed. One basic requirement for qualification testing is therefore to test the component under conditions as close to the real life as possible and practical, while applying the different accelerated loads in “real” succession. As an example, as part of qualifying a hydraulic coupling, this should be mounted as in its intended life to reveal any adverse effects from the locking system.

All components shall as far as possible be qualified against standard functional requirements compatible with the criticality of the component.

“Test to failure” should be performed whenever practical to establish the real limitations of the component.

C.3.7 Summary of component testing

The qualification based on component testing as described in this section applies to standard mass-products and simple items, i.e. hydraulic pipefitting. All of the parts described above are covered in the Recommended Practice, although this outline does not fully cover the extensive development of a Technology Qualification Basis, identifying all the different uses.
C.4 A subsea multiphase pump; Kværner Eureka

C.4.1 Multiphase pump

C.4.1.1 Example

This example focuses on different aspects of the Technology Qualification Process. The unit is installed on the seafloor for multiphase (arbitrary mix of gas and fluid) pumping from a hydrocarbon reservoir drained through subsea wells.

The pump is equipped with auxiliary components and systems such as a pressure and volume compensation system (a compensator), a cooling system, filters, instrumentation, penetrators, etc. All components are mounted on a skid and placed in a dedicated subsea module frame.

The selected example is qualification of the diaphragm in the compensator. (In this case a steel bellows).

C.4.1.2 Scope of this example

The purpose of the following is to outline the application of the Recommended Practice for:

— check list for Technology Qualification Basis
— failure mode and mechanism identification for a limited area (the bellows)
— reliability data collection for the bellows.

The latter focus on alternative approaches is dependent on the types and quality of the available documentation.

C.4.2 Applied data

The technical data used is mainly based on general information available in handbooks, on the internet and brochures.

C.4.3 Technology Qualification Basis Check list

The purpose of the checklist is to keep a clear trace of the parameters to be used for the qualification, and including possible changes.

The checklist should include all parameters that describe the requirements for the equipment. Examples of such parameters are:

— specifications (quantified) such as
  — intended function of the equipment, e.g. capacity
  — lifetime, e.g. target service time, number of cycles before failure
— loads
  — mechanical
  — thermal
— operating conditions
  — operating pressure (range)
  — temperature (range)
  — environment.

Table C-6 illustrates a typical checklist for the Technology Qualification Basis.

C.4.4 Ranking of failure modes

C.4.4.1 Definitions of probability and consequence values

The subsea multiphase pump module has been subject to a failure mode effect and criticality analysis (FMECA) using the following categories:

*Probability categories:*

<table>
<thead>
<tr>
<th></th>
<th>Probability Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Medium</td>
</tr>
<tr>
<td>3</td>
<td>High</td>
</tr>
<tr>
<td>4</td>
<td>Very High</td>
</tr>
<tr>
<td>5</td>
<td>(Not included)</td>
</tr>
</tbody>
</table>

Failure within 10x service life unlikely
Failure within 10x service life possible, but unlikely within service life
Failure within service life likely
Several failures within service life likely
Frequent failures within service life likely
Consequence categories

1. Low Equipment failure that does not cause production loss - no pollution
2. Medium Equipment failure that is not critical, repair can wait until next intervention - no or minor pollution
3. High Equipment failure that is critical, requires controlled shut down. Production loss without equipment damage - no or minor pollution
4. Very High Equipment failure that is very critical, requires that the equipment must be replaced, production loss, possible pollution.
5. (Not included)

For the purpose of this limited demonstration on the bellows, four categories were found to be practical.

C.4.4.2 Determination of risk

C.4.4.2.1 Failure of modes of concern

The analysis showed that the function of the compensator was critical for the main functions of the module, and that the function of a diaphragm located inside the compensator would be critical for the intended function. Table C-8 shows the results of the FMECA of the bellows.

The consequence of failure of the bellows is that the pressure compensator cannot perform its intended task, which in turn can lead to failure of the pump seal and breakdown of the pump, i.e. consequence category; 4 very high.

The probability that the identified damage mechanisms will occur and will cause failure within the defined service life of the bellows is initially determined to be low to medium (probability categories 1 low to 2 medium). There are several routes to go for obtaining the reliability data, and the uncertainty can be reduced to arrive at an acceptable risk level, as shown in the following, for the bellows.

C.4.4.2.2Failure mechanisms of concern

Main failure mechanisms are governed by:

- material fatigue
- buckling
- corrosion
- fretting
- deposits.

The bellows are in general very sensitive to defects like dents, scores and to twisting. Handling during assembly can cause this. If defects or twisting exist, the probability that this will cause failure within the design lifetime of the bellows has been judged to be high, initial probability category; 3 high. Appropriate procedures for handling, mounting and inspection, and for qualification of personnel can reduce this category.

Other more general, but important aspects are:

- the damage tolerance of the design (robustness)
- possible deviations from nominal conditions
- the manufacturer's experience background
- qualification effort put into the design and testing of the design
- the quality of standards applied in design and manufacturing.

These are further dealt with in the following.

C.4.5 Reliability data collection

C.4.5.1 Planning

The objective is to provide sufficient data of good enough quality for evaluating the system reliability with regard to the most critical failure modes and consequences.

Data collection will aim at collecting the data that describe the probability that a failure mechanism will develop until damage. This implies also the aim at reducing the uncertainty in data or at getting a better understanding of how uncertain the actual data are.

A stepwise approach is applied with the aim to provide the necessary and sufficient basis with a minimum of efforts.

C.4.5.2 Technology Qualification Basis for the Compensator - Bellows

C.4.5.2.1 Design

The following example will focus on the bellows, and consider the rest of the pump module only as a set of boundary conditions.

The diaphragm consists of a bellows, springs, an end plate (piston) and guiding.
The following figures are copied from the Witzenmann GmbH brochure. They illustrate typical use and design of bellows.

The bellows is made from 4 plies of Inconel 625 sheets of 0.3 mm thickness, which are rolled and welded to cylinders that fit into each other, and then expanded into the final corrugated shape.

**Figure C-4**
A sketch of a bellow installed in a pressure housing, and the clamping of the bellows to the solid structure

---

**C.4.5.2.2 Number of operations**

There has been defined a target lifetime for the bellows in terms of years in service and the anticipated number of typical load cycles during that period. The design lifetime of the bellows in terms of load cycles is ten times the number of full load cycles anticipated during its target lifetime. Two types of load cycles have been defined, the full stroke cycle and the 10% stroke load cycle. For every full stroke load cycle one anticipates that 20 load cycles of 10% of full stroke will occur. This definition is considered to cover actual strokes with respect to fatigue life.

**C.4.5.3 Fatigue - The stepwise approach**

The stepwise approach related to material fatigue damage consists of the following main sources of data:

1) Material fatigue strength represented by strain-number of cycles curves or stress-number of cycles curves (S-N curves), in this case correlated with one actual test.

2) Crack initiation.

3) Crack growth.

   Further is considered:

4) Damage tolerance.

5) Deviations from nominal conditions.

   The alternative, which depends on its quality is represented by

6) Standards and Experiences.

Design according to the above item 6 alone could give the desired reliability. Uncertainties with respect to the standard could, however, lead to separate investigations as indicated by item 1 to 3 and supplemented with item 4 and 5.

The items are further detailed in the following:

**Lifetime evaluation level 1**

**Fatigue lifetime evaluation based on S-N curves:**

Lifetime evaluation level 1 - Fatigue lifetime evaluation based on S-N curves:

S-N curves are usually based on data from fatigue test specimens, and represent a stated probability of specimen survival at the strain-range and number of load cycles. For stresses below the yield limit, the strain-range is proportional to the stress-range. The observed fatigue life includes crack initiation, crack growth and final fracture of the specimens, which often are cylindrical rods of a diameter of 6.27 mm. Use of S-N curves has limitations for evaluation of fatigue lifetime of actual constructions, in particular if the geometry is very different from that of the test specimens, as the case with this multi-layer bellows.

S-N curves can be used for evaluating if the probability of fatigue of the bellows is higher than desired under the given conditions.

If fatigue life of the bellows is infinite for the most severe strain-range encountered in use (full stroke), the probability of fatigue failure is so low that the fatigue evaluation can be concluded at this level. The evaluation of damage tolerant design (see lifetime evaluation level 4) still has to be carried out. Otherwise the fatigue evaluation has to be continued by evaluating the probability of crack initiation (lifetime evaluation level 2).
Detailed example:

Stress and strain data for the bellows are not made available. Lifetime calculation by use of S-N data is thus not possible. However, one prototype bellows has been tested at full stroke, and survived 20 times the design number of full stroke cycles with no indication of failure or fatigue crack initiation. This test result can be used in a lifetime evaluation, e.g., will more tests be required to ensure that the probability of fatigue failure under defined service conditions is acceptable.

The following information is available:

— S-N curve for Inconel 625 (in a Log S - Log N format):
  
  In the region of interest, the S-N curve is of the form
  \[ \log(N) = \log(a) - m \cdot \log(S) \]
  where
  
  \[ N = \text{the mean number of cycles to failure under strain-range } S \]
  \[ S = \text{strain-range} \]
  \[ a = \text{a constant relating to the mean S-N curve} \]
  \[ m = \text{the inverse slope of the S-N curve} \]

— The scatter in the observed cycles to failure at a given strain-range can be described by a normal distribution on the Log N axis, and the standard deviation of Log N is Log s.

— DNV-RP-C203 - Fatigue strength analysis for mobile offshore units - gives typical values for Log s in the range 0.18 to 0.25. For the geometry of the bellows Log s = 0.2 will be relevant.

— The prototype bellows has been tested at 20 times the design number of full stroke cycles with no indication of failure or fatigue crack initiation.

Furthermore, the following assumptions are made:

— Tests of specimens of Inconel 625 would give a scatter in the observed lifetimes similar to that of steel in cleaned, as-rolled condition, i.e. Log s = 0.2.

— Only full stroke cycles (as specified in the Technology Qualification Basis) affect the fatigue life.

The S-N curve for Inconel 625 is shown in Figure C-5 with number of cycles N as x-axis and strain-range as y-axis. The design number of cycles, 500 cycles, is marked with an open triangle, and the prototype test result is marked with a filled triangle. Since there is only one test result available, the mean S-N curve is drawn through this point as a first assumption.
To get a better basis for evaluating, if more fatigue tests are required, assume as shown in Fig.C-6 that the test result is much better than average and corresponds to a lifetime three standard deviations better than the mean lifetime. This is a very conservative assumption, as it implies that the probability that the test result is even better than assumed, at only 0.135%. The mean lifetime is then 2512 cycles (Log 10000 = Log N + 3 \cdot \log s; Log N = 4 - 3 \cdot 0.2 = 3.4). As shown in Fig.C-6 the design number of cycles is well below three standard deviations below the mean lifetime (Log (N - 3s) = Log N - 3 \cdot \log s = 3.4 - 3 \cdot 0.2 = 2.8; N - 3s = 631 cycles). Based on the above assumptions, the probability of failure at 631 cycles will be 0.135%, and the probability of failure at 500 cycles will be even lower than that.

Based on the above reasoning, and the fact that the bellows survived 10000 cycles without visible failure damage, one can conclude that failure of the bellows due to fatigue is very unlikely.

**Guidance note:**

ISO FDIS 2394:1998(E) D.5.3 - Partial factor design: Bayesian method describes a method for calculating the design value given a desired probability of failure, one or more test results and a known or, in case of more test results, calculated standard deviation.

A similar approach can also be applied for failure mechanisms described by distribution functions visualised on graphs with linear scales, or any type of scales, e.g. by the X axis as a linear time scale and number of standard deviations with linear relation. See “Guide to the expression of uncertainty in measurement, ISO 1995” which defines “experimental standard deviation” “\(s_t\)” from measurements as:

\[
s_t^2(q_k) = \frac{1}{n-1} \sum_{k=1}^{n} (q_k - \bar{q})^2
\]

\(q_k\) = measured value  
\(\bar{q}\) = mean value of measurements  
\(n\) = number of measurements  
\(k\) = measurement no

For information, a typical normal distribution function is shown in **Figure C-7**.
Lifetime evaluation level 2

Fatigue lifetime evaluation based on the probability of crack initiation:

S-N curves for crack initiation are usually not available. The approximate position of such curves can be derived from basic knowledge of the material used and from crack growth data for this material.

S-N curves for crack initiation can be used for evaluation if fatigue crack initiation is probable under the given conditions.

If crack initiation is probable for the most severe stress range, crack growth due to this stress range and also other relevant stress ranges must be evaluated.

Lifetime evaluation level 3

Fatigue lifetime evaluation based on crack growth:

If crack initiation during the target lifetime has to be taken into account, the probability of through cracks has to be evaluated. Both the most severe stress range and other relevant stress ranges have to be considered.

Use of fracture mechanics and relations of the type can calculate crack growth

\[ \frac{da}{dN} = C f(\Delta K) \]

where

- \( a \) = crack length at the moment
- \( N \) = number of cycles
- \( C \) = material constant
- \( \Delta K \) = cyclic stress intensity factor range

Several versions of such relationships exist, the most well known being the Paris equation, see e.g. H. O. Fuchs and R. I. Stephens “Metal Fatigue in Engineering” or other textbooks on fatigue.

This allows calculation of the relative contribution to crack growth from other load cycles than the most severe load cycle, and, when the threshold for crack growth is known, determination of the crack size at which crack growth changes from crack initiation to much faster fatigue crack growth.

Crack growth is an important aspect in determining the interval between inspections, i.e. the safe period of operation after installation or intervention (inspection).

Lifetime evaluation level 4

Damage tolerance

Lifetime evaluation has been carried out for the bellows in nominal condition, i.e. the geometry of the bellows, the load situation etc. are as given in the description of the bellows.

In addition to this, the damage tolerance of the design should be checked. This means that the effect of possible flaws from manufacturing and assembly are to be estimated, and also possible damage during operation, e.g. formation of pits due to corrosion, fretting, etc. that can act as initial cracks or stress-raisers.

Lifetime evaluation level 5

Evaluation of deviations from nominal condition

The above evaluation is based on nominal conditions, i.e. that the geometry of the bellows, the load situation etc. is as are as given in the description of the bellows. The effect of possible (reasonably probable) deviations from this should also be checked, e.g.

- manufacturing and assembly tolerances, including deviations from axi-symmetric conditions
- excessive loads that can be caused by not typical operating conditions, malfunction, etc.

The latter shall be specified in the Technology Qualification Basis.
**Details of example:**
The fabrication process should be reviewed with regard to tolerances to be specified. It is known that loading a bellows in torsion (twisting) in general produces extremely high shear stresses and can greatly reduce both fatigue life and pressure capacity. The maximum allowable torsion moment should therefore be identified, and checked that the possible actual torque is well below.
The design of the axial bellows guidance, effects from possible springs (including spring breakage) and the assembly procedure of the compensator should address the effect on the torque. The above items will be input to the qualification of the design of the compensator and to the qualification other components of the compensator.

**Lifetime evaluation level 6**

*Evaluation of the manufacturer’s data, criteria, calculations, testing, experience, standards used*
The design of the bellows can be based on a standard. In this context the background for the standard with respect to life time estimates should be documented and qualified. If not, qualification of the standards with respect to the implicit probability of failure must be carried out.

*Details of example:*
The manufacturer of the bellows for the compensator designs and manufactures bellows according to the “EJMA” standard (Expansion Joint Manufacturers Association, Inc. 1998). This standard says that the average fatigue lifetime is equal to the or higher than the design lifetime. DNV experience indicates that the lifetimes observed in fatigue tests of bellows are usually well above the design lifetime.
The compensator bellows can also designed according to a proprietary standard developed by the manufacturer. According to this, the bellows has a calculated lifetime above the design lifetime. The manufacturer states that his standard is accurate and more conservative than the EJMA standard. Since no documentation on this is available, it is difficult to evaluate what the calculated lifetime implies in terms of probability of failure, e.g. if this corresponds to 30%, 10% or some other probability of failure. Consequently the additional evaluations given in level 1 is required.

**C.4.5.4 Buckling**

Buckling of the bellows could cause functional failure of the compensator by hindering the required motion of the bellows. Buckling is not acceptable within the lifetime of the bellows.

Specification of long lifetimes (high number of cycles) can result in a bellows, which is highly flexible and could have reduced stability under pressure.

The EJMA standard also addresses the stability of the bellows by formulas and criteria. In this case a guide is used for preventing radial motion and thus buckling of the bellows.

The probability of failure due to instability is considered to be low.

**C.4.5.5 Corrosion**
Pitting corrosion could be critical. The pits that can act as stress raisers and or initial cracks. Fatigue cracks can grow from such pits. Because each ply is only 0.3 mm thick, corrosion pitting can penetrate an outer ply of the bellows and allow corrosion attack of the inner plies as well, causing leakage.

Pitting corrosion is not acceptable within the lifetime of the bellows. Material selection and control of the environment should be used to control this failure mode.

Since both the system fluid and the fluid in the compensator housing have low corrosivity, the probability of corrosion attack on the bellows is evaluated as low under normal operating conditions.

If the fluid in the housing is polluted by produced fluid, the fluid outside the bellows will become corrosive. According to established service experience in H₂S service, Inconel 625 has proven not susceptible to corrosion when the surface hardness ≤ 35 HRC. Pitting is not reported to be a problem.

The flange material is corrosion resistant. Further general corrosion of the flange is not a problem because of the thickness.

**C.4.5.6 Fretting**

Fretting could be critical since it can cause pits that can act as stress raisers and or initial cracks. Fatigue cracks can grow from such pits. Fretting could occur between the plies and cannot be detected by visual inspection.

Fretting is not acceptable within the lifetime of the bellows.

Fretting wear occurs form repeated shear stresses that are generated by friction during small amplitude oscillatory motion of sliding between two surfaces pressed together in intimate contact. Surface cracks initiate in the fretting wear region. The relative slip amplitude is typically less than 50 μm. Fretting wear increases linearly with contact load.
There seems to be a possibility that conditions that can cause fretting wear may exist somewhere in a multi-layer bellows. Data for evaluating this are not available, and criteria for fretting wear are vague. It is not possible to arrive at any conclusion based on available data.

Fretting is not addressed in the EJMA standard. DNV have not recorded bellows failures due to fretting. Fretting is most probably not a problem in bellows, but there is some uncertainty about this. This should be followed up by inspections after test.

C.4.5.7 Accumulation of deposits on/around bellows

Accumulation of deposits on or around the bellows can cause functional failure of the compensator by hindering the required motion of the bellows.

The effects from the environment must be examined. It is assumed that this is only of concern in case wax or hydrates can form, or sand settles on the one side of the bellows, or contamination of the clean fluid on the other side.

Therefore a study should be carried out for the purpose of determining that the risk for deposit accumulations is acceptably low.

C.4.5.8 Conclusions

The above demonstration shows that conclusions regarding the reliability of components with regard to critical damage mechanisms can be made even when data are sparse or lacking. The evaluation points to areas where better data is required.

Standards used for designing may be based on reliability considerations or on experience regarding designs that have functioned acceptably in service. If standards are documented and verified, comparing with the standards can assess the reliability of the components. If such standards are proprietary or not verified they are of less value for reliability assessment.

Results of tests, even though the number of tests is far from statistically significant, can facilitate sufficient background for reliability evaluation when combined with relevant other data than those from tests alone.

C.4.6 Maintenance and modifications

The cost of an intervention of the sub sea multiphase pump module is so high that unscheduled interventions must be avoided. This means that all parts of the multiphase pump module must have a minimum lifetime equal to or longer than the time between scheduled interventions. The cost of replacing parts and components at the intervention is marginal compared to the cost of carrying out the intervention. This means that the pump must be replaced with a new or overhauled pump module. The overhauled module parts that are subject to wear or deterioration have been replaced. Because unscheduled intervention is extremely costly, it is of importance to detect conditions that could require intervention early to allow time for planning. On the other hand, false indications cannot be accepted because of the costs.

Because the sub sea multiphase pump module is new technology in the sense that it has not a record of previous successful use subsea, intervention for replacement is planned at regular intervals. The design lifetime of the bellows is the same as the target interval between interventions.

The analysis of the bellows shows that the probability for failure within this interval is so low that no additional inspection or maintenance is required, provided that the bellows is assembled correctly according to the “right” procedures and that no indications of defects were found at the subsequent inspection.

The function of the compensator could be monitored by a system that continuously measures the position at the end of the bellows. This will also serve as condition monitoring of the bellows, since lack of movement or irregular movement will signal that there is a problem. Higher sensitivity can probably be achieved by correlating the movement of the bellows with other parameters such as pump inlet pressure.
Table C-7 Specifications for the subsea pump module

<table>
<thead>
<tr>
<th>Specifications - Subsea Multiphase Pump Module</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Design life time pump module</strong></td>
</tr>
<tr>
<td>Design life pump module</td>
</tr>
<tr>
<td>Design time between intervention</td>
</tr>
<tr>
<td>Design load full amplitude cycles of bellow between intervention</td>
</tr>
<tr>
<td>Design load 10% amplitude cycles of bellow between intervention</td>
</tr>
<tr>
<td><strong>2. Operating Environment</strong></td>
</tr>
<tr>
<td>Ambient conditions – storage</td>
</tr>
<tr>
<td>Minimum air temperature</td>
</tr>
<tr>
<td>Maximum air temperature</td>
</tr>
<tr>
<td>Ambient conditions – submerged testing</td>
</tr>
<tr>
<td>Maximum water depth</td>
</tr>
<tr>
<td>Minimum water temperature</td>
</tr>
<tr>
<td>Maximum water temperature</td>
</tr>
<tr>
<td>Ambient conditions – at subsea location for operation</td>
</tr>
<tr>
<td>Maximum water depth</td>
</tr>
<tr>
<td>Minimum water temperature</td>
</tr>
<tr>
<td>Maximum water temperature</td>
</tr>
<tr>
<td>Installation</td>
</tr>
<tr>
<td>Wave height</td>
</tr>
<tr>
<td>Maximum landing velocity</td>
</tr>
<tr>
<td>Maximum horizontal acceleration</td>
</tr>
<tr>
<td><strong>3. Pumped medium specifications</strong></td>
</tr>
<tr>
<td>Maximum fluid temperature at wellhead</td>
</tr>
<tr>
<td>H₂S content in gas phase</td>
</tr>
<tr>
<td>Carbon dioxide in well stream</td>
</tr>
<tr>
<td>Oxygen</td>
</tr>
<tr>
<td>Acidity</td>
</tr>
<tr>
<td>Average sand content (weight)</td>
</tr>
<tr>
<td>Maximum sand particle size</td>
</tr>
<tr>
<td><strong>5. Pump parameters</strong></td>
</tr>
<tr>
<td>Design point</td>
</tr>
<tr>
<td>Suction pressure (for a specific application)</td>
</tr>
<tr>
<td>Discharge pressure (for a specific application)</td>
</tr>
<tr>
<td>Design pressure</td>
</tr>
<tr>
<td>Hydrostatic test pressure</td>
</tr>
<tr>
<td>Suction temperature (for a specific application)</td>
</tr>
<tr>
<td>Gas flowrate (A - ambient)</td>
</tr>
<tr>
<td>Liquid flowrate</td>
</tr>
<tr>
<td>Total flowrate</td>
</tr>
<tr>
<td>Gas void fraction</td>
</tr>
<tr>
<td>Gas density</td>
</tr>
<tr>
<td>Liquid density</td>
</tr>
<tr>
<td>Total density</td>
</tr>
<tr>
<td>Pump speed</td>
</tr>
<tr>
<td>Pump shaft power</td>
</tr>
<tr>
<td>Maximum operating point</td>
</tr>
<tr>
<td>Total flowrate at 40 bar differential. pressure</td>
</tr>
<tr>
<td>Pump speed</td>
</tr>
<tr>
<td>Pump shaft power</td>
</tr>
<tr>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>ID</td>
</tr>
<tr>
<td>-----</td>
</tr>
<tr>
<td>2.1</td>
</tr>
<tr>
<td>2.2</td>
</tr>
<tr>
<td>2.3</td>
</tr>
<tr>
<td>2.4</td>
</tr>
<tr>
<td>2.5</td>
</tr>
</tbody>
</table>
APPENDIX D  COMPUTER SOFTWARE

D.1 Introduction

This section describes the process for Technology Qualification of computer software, either as an independent system or as part of a larger system. Software may be provided in many applications, including:

— computational and data processing systems, not controlling hardware
— software that controls specific physical devices
— software in networks linking devices and computational systems.

This annex addresses Technology Qualification in all of those types of application.

While the qualification of hardware may be accomplished on the basis of the detailed design that is provided to the manufacturer, the detailed design of software usually is not adequate for this purpose. Many performance and behavioural aspects of software cannot be evaluated until code has been developed and executed.

Because software does not go through a manufacturing phase (where further product improvement is possible), it is essential that software quality and technology qualification issues be addressed during initial software development and testing. Most of the planned investment in a new software capability is expended in producing the first copy.

Unlike software, the creation of each additional copy of a hardware device requires a significant investment in manufacturing the new copy. Additional copies of the software are nearly “free”, although they may contain “bugs” which are likewise easily propagated. Software bugs are not discovered during software “manufacturing”.

Technology qualification differs from traditional software quality assurance in that qualification stresses risks, not just requirements, and attempts to produce a quantitative statement of confidence in the finished product. However, many of the same techniques are used.

These recommendations for Software Technology Qualification builds upon established guidance. International standards describe the typical dimensions of software quality (ISO/IEC 9126) and generic software development processes (ISO/IEC 12207). The guidance in this annex employs many of the key concepts of those standards. App.[D.2] outlines the overall process of Software Technology Qualification. It parallels the steps of the Technology Qualification Process described in the main body of this recommended practice. App.[D.3] discusses some software-specific issues that often surface during Software Technology Qualification efforts.

D.2 Technology Qualification Process

The Software Technology Qualification Process consists of six steps, as described below. App.[D.2.7] discusses concept improvement based on the Technology Qualification results.

D.2.1 Technology Qualification Basis

Technology Qualification attempts to substantiate a Claim about provision of function. The first step in qualification is to define the technology specification or basis for qualification. Unfortunately, software requirements often are embedded in other systems requirements, rather than being identified separately. Consequently, it may be necessary to consolidate information from many sources in order to build the software technology specification. The software technology specification may be a collection of data, rather than a formal document.

Most guidelines for development of software-intensive systems recommend that a functional allocation of requirements to software and hardware components be developed. If available, that is a good starting point for the development of the software technology specification. Other potential sources of qualification criteria include the following:

— operations concept
— functional requirements
— performance requirements (throughput, CPU utilization, responsiveness)
— definitions of interfaces and dependencies
— acceptance criteria
— quality and service level objectives
— applicable industry standards (e.g., ISO 61508 for safety-critical systems).

The technology specification should itemize all features, capabilities, and qualities that affect the ability of the software to perform its intended functions effectively. These are the qualification criteria. Don’t assume that the formal requirements document developed by the customer or supplier contains all of this information. The technology specification should include a functional architecture, that is, a mapping of qualification criteria to functional components of the system.

Because it is practically impossible to exhaustively test any software of substantial size, developers should
employ a systematic approach to verification and validation that incorporates methods other than testing, as well. Not all qualification criteria may be tested or testable. Other verification methods may be used as discussed below. Technology qualification provides an overall assessment of fitness for purpose using all of the available and appropriate data.

It may be helpful to clarify some software terminology used later in this document:

— Failure – occurs when the software operates in a way that fails to meet its requirements or expectations (these are identified through testing and usage).
— Defect – something in the code or documentation that must be changed in order to correct the failure (these are identified through peer reviews and debugging).
— Problem – a report or record of one or more failures and/or defects.

These terms are used loosely in practice. Problem is the most general term.

The quality dimensions defined in ISO/IEC 9126 often are a useful way of organizing a software technology specification to ensure that all important software quality attributes are covered by the specification.

A desired Confidence Level (DNV-RP-D201) or Safety Integrity Level (IEC 61508) may be established during this step. These standards define four levels of increasing confidence and/or safety. The Technology Qualification effort should determine whether or not the necessary level of reliability and other performance measures has been achieved to meet the selected Confidence Level or Safety Integrity Level.

D.2.2 Technology Assessment

A formal Technology Qualification Process is recommended for technology that is not covered by a set of validated requirements. This step determines the scope of the Technology Qualification effort. Software packages that are used for their original purpose in the intended environment without modification generally do not require Technology Qualification.

This Recommended Practice provides a general algorithm for assessing technology. The following recommendations are provided specifically for software elements. New software shall be categorized as “novel or unproven” (see Table in Sec.7.4) to determine the need for qualification. Rate substantially modified software as “limited field history” in the same table. Each software component should be considered separately. Thus, some software components may require qualification, while others do not.

Technology Qualification may begin with software design information. However, many important aspects of software behaviour will not be known until software code has been developed and tested. As discussed in App.[D.3.5], one or both of the design and source code may not be available for COTS and legacy software. Qualification for these components will have to be based on the behaviour of the software observed during testing.

D.2.3 Threat Assessment

Once the Technology Qualification Basis has been created, risks to achieving the qualification criteria should be identified. This can be accomplished by combining a system-level risk analysis with FMECAs for selected software components, as appropriate. Risk analysis activities help to focus the verification and validation activities of the technology qualification team. (The qualification team includes facilitators, vendors, and customer personnel contributing to the qualification activity.)

The system-level risk analysis should be conducted using the DNV analysis method and supporting tools (e.g., Easy Risk Manager). The first steps are to develop a risk taxonomy as well as criteria for rating the probability and consequence of risk items. The functional architecture forms one dimension of the risk taxonomy. The system-level risk analysis should address a broad range of possible obstacles and risks associated with the technology, including processes, personnel, infrastructure, and regulatory concerns. It should not be limited to the scope of the software. Easy Risk Manager provides good support for capturing and tracking the results of the risk analysis.

Software FMECAs focus on individual software-controlled devices, usually identifiable in the functional architecture. The system-level risk analysis may identify some system components as problematic, and thus appropriate for further consideration in a software FMECA. Software should be included in the FMECA for any system component where software can initiate or inhibit any safety action, even if hardware barriers appear to be independent of the software. If the schedule allows, individual software components should be qualified before they are integrated into the system.

Threat keywords may be helpful in recognizing potential problems during risk analysis and FMECAs. Examples of such keywords for software include: requirements changes, buffer overflow, memory leaks, manual processes, global memory, reuse, timing constraints, Java, Visual Basic, hard-coded parameters, and fault tolerance.

Whenever technology that requires qualification is implemented in a system that integrates hardware and software, with a high required level of confidence, then DNV-RP-D201 should be applied, as well. The largest benefits result from applying DNV-RP-D201 early in the project. A gap analysis based on DNV-RP-D201 helps to identify weaknesses in the development process that may allow defects to escape into the software.
Addressing these weaknesses helps to reduce the probability of occurrence of such failures generally, not the likelihood of any specific failure. The risk analysis and FMECA activities typically carried out during qualification of software identify specific potential failures to be mitigated. DNV-RP-D201 can be applied at project start (for example, during vendor selection) before the requirements, architecture, and design documents that are needed for the detailed FMECAs in the Technology Qualification Process according to this RP are available. Thus, DNV-RP-D201 is complementary to this one.

Figure D-1 shows the relationship of these Recommended Practices to Technology Qualification. Just DNV-RP-A203 provides process guidance to the TQ effort, DNV-RP-D201 provides guidance to the software development effort and also provides information to the TQ team about the verification data likely to be available.

![Figure D-1](image)

**Figure D-1**
DNV Recommended Practices Related to Technology Qualification

### D.2.4 Develop Technology Qualification Plan

The Technology Qualification Plan describes the data to be collected and analyses to be performed to qualify the software. The “must have” software requirements, high priority risks, and critical failure modes (identified as described in App.[D.2.3]) indicate the kinds of data required for the qualification effort. Appropriate data must be collected to determine if the requirements are satisfied, risks have been mitigated and barriers to failures are successful. A Software Technology Qualification effort may incorporate data from many different sources within a project. In particular, quality assurance, verification, and validation activities that projects normally undertake can provide valuable data for qualification. The Technology Qualification Plan should identify the data to be collected from the software development process, as well as the analyses to be performed on it. The plan should also describe any activities necessary to obtain needed data that is not produced naturally within the developer’s process. The ability of the developers’ process to produce the desired data can be determined via a DNV-RP-D201 process assessment. IEC 61508, Part 3, recommends verification activities for differing Safety Integrity Levels.

The Technology Qualification Plan must identify an appropriate verification and validation strategy for each high priority requirement, risk or failure mode. Qualification typically involves data from the following sources:

- Peer review results:
  - number of defects found
  - location and type of defects.

- Problem reports from testing:
  - number of defects found and fixed
  - location and type of defects.

- Test evaluation reports:
  - functionality gaps
  - test coverage.

- Source code analysis results:
  - complexity
  - violations of standards.
— Technical performance measures:
  — memory utilization
  — response time
  — throughput
  — CPU utilization.

The Technology Qualification Plan should identify the qualification criteria, data to be collected, and analyses to be performed. Ideally, the software acquirer and developer perform these activities and make the data available for the qualification analysis. If that is not true, then consider making these activities part of the software technology qualification effort. Each activity in the Technology Qualification Plan should be linked to a corresponding requirement, risk, or failure mode(s).

A baseline assessment of suppliers’ processes should be conducted to identify their quality activities and data that might be made available for the qualification analysis. DNV-RP-D201 provides a framework for conducting such an assessment. The baseline assessment should produce an evaluation of the effectiveness of the supplier’s verification and validation activities (with recommendations for improvement), as well as a list of data items to be considered in the qualification analysis. Particular attention should be paid to the problem tracking and corrective action systems in use.

Problem reporting systems are an important source of information for technology qualification. These systems track problems found during peer reviews and testing. Developers rely on these systems to ensure that the identified problems get resolved in a timely manner. The technology qualification activity can use this information to help to determine how well the technology specification is being satisfied and the project quality trends – for example, through the use of reliability models, as discussed later. A description of each problem or defect should be recorded, along with information such as:

— Location in the software (module) or test case where the problem was found.
— Severity (impact) and or priority of problem.
— Type or nature of the problem.
— Status of problem (open, in work, closed).
— Planned fixed (release or date to be delivered).

Maintaining the integrity of the problem reporting system is essential to both the project’s quality assurance activity and the technology qualification effort.

Source code analysis involves processing the source code through a software tool to identify potential problems and quality issues. This is also referred to as static code analysis because the software is not being executed, as it would be during testing. Not all problems can be detected with static code analysis. The types of problems source code analysis tools may find include:

— Control flow – unreachable code, and loops with multiple exit or entry points.
— Data use – variables used without being initialized and variables declared but never used.
— Interfaces – inconsistencies in the variables passed between two routines, such as incorrect number of variables passed or inconsistent variable types.
— Memory leaks – failure to de-allocate storage after use.

Other types of errors, e.g., mistakes in algorithms or logic cannot be detected by source code analysis. Source code analysis also gives insight into the structure and format of the code that may help to improve its maintainability.

Many source code analysis tools are available, both free and commercially. Refer to this website: http://en.wikipedia.org/wiki/List_of_tools_for_static_code_analysis.

Some aspects of software, especially algorithms, may be verified through formal methods. These are tools and techniques (e.g., Z) that can prove that software is correct with respect to its functional requirements. Typically, formal methods are employed by the developer, not as an after-the-fact verification technique. However, evidence of the use of formal methods may be considered during the technology qualification effort. Formal methods generally do not address performance-related problems.

Technology qualification focuses on the new or innovative aspects of a system or product. The project team may apply conventional testing and quality assurance activities to a broader scope of the project than is relevant to the novel technology. Technology qualification applies a more rigorous quality approach to the novel technologies within the system.

**D.2.5 Execute Technology Qualification Plan**

This step consists of executing the plan described in the preceding section. Changes to the plan may be required if some of the planned data cannot be obtained. Ideally, the software development team performs the activities needed to generate the qualification data as part of their normal activities.
D.2.6 Performance Assessment

This step involves collating results and further analyzing data collected through the execution of the Technology Qualification Plan. The results of this step are documented in the Technology Qualification Report. However, status reports, showing progress towards qualification, may be provided at defined milestones. As discussed in App.[D.2.2], qualification may begin with software design, but final qualification requires results from software testing.

Ideally, the qualification report should be developed jointly among all the stakeholders. However, sometimes concerns for proprietary data make that impossible. The qualification report should contain the following items, as a minimum:

— Qualification criteria (the Technology Qualification Basis):
  — acceptance criteria
  — technical performance measures
  — quality objectives
  — risk analysis results.

— Sources of qualification data:
  — acquirer-supplied items
  — vendor-supplied items
  — qualifier-supplied items.

— Assessment of satisfaction of qualification criteria:
  — gaps
  — uncertainties.

— Recommended actions:
  — risk mitigations
  — corrective actions
  — further evaluation/qualification.

— Projections of reliability and maintainability in operation (See App.[D.3.7])
— Projected lifetime until obsolescence (See App.[D.3.3] and [D.3.4]).

A thorough review of the qualification report by all stakeholders is recommended before finalization to ensure an accurate interpretation of the data.

D.2.7 Concept Improvement

As a result of risks identified during the threat assessment or problems and unresolved risks identified during the Performance Assessment, improvements to the software design and implementation may be needed. During the Concept Improvement step these issues are communicated to the software developers. The Technology Qualification team may collaborate with the software developers in defining corrective actions. Depending on the nature of the issues and corrective action, some qualification steps may need to be repeated.

D.3 Special Topics

This section identifies some of the software-specific concerns that should be considered in a Software Technology Qualification effort. These concerns may not all be important in every situation.

D.3.1 Maintenance and Modification Effects

Software Technology Qualification may be conducted during initial system development, or later during operations when technology is introduced into a system. Regardless of when conducted, the qualification activity should consider the maintenance and modification of software during operations. Software should be designed for maintainability. Software changes arise from many sources:

— planned enhancements to functionality
— fixes to correct problems
— updates to operating systems, databases, and other packages incorporated into the system.

Managing changes efficiently and effectively is essential to manage system availability during operations. Typical maintenance-related qualification criteria include the following:

— How difficult is the software to change?
— How many latent defects are likely to be present in the software?
— Does the vendor have the resources and commitment to maintain the software (work-off the defect backlog) through its expected life?
— How much does maintenance and support after delivery cost?
— Are the operating systems, databases, and other packages incorporated in the system stable?

Source code analysis tools may be an effective way to assess the difficulty of modifying the software. These software packages process the source code to map its structure and measure its complexity — key factors in maintainability. They can also help to identify the impacts of potential changes to the software.

Reliability analysis (App. [D.3.7]) discusses techniques for estimating the latent defects and monitoring the work-off of the defect backlog. Defect causal analysis may be employed to help identify systematic weakness in the system design as well as development and maintenance processes. This approach helps reduce the cost of maintenance by preventing additional defects.

Unlike hardware, software does not wear out. Thus all the defects and potential failures that software might experience are delivered with it, unless more are added during maintenance. Any software change that affects an identified threat or failure mode should be re-verified to ensure that the risk is still handled correctly.

The amount of maintenance required by software does not necessarily increase with age. The decision to retire and/or replace software tends to be driven by supplier actions such as major changes to operating systems, databases, and other packages incorporated in the system, increases in the price of maintenance support, or by the need to add new functionality that cannot easily be accommodated by the existing software system.

D.3.2 Fault tolerance

Fault tolerance is the ability of a system to continue operating in the presence of faults or failures. The level of fault tolerance achieved in a system usually depends on the system architecture. Often, fault tolerance is achieved through redundancy. This means having multiple capabilities for performing the same function, typically in parallel. ISO/IEC 42010:2007, “Systems and Software Engineering — Recommended practice for architectural description of software-intensive systems”, suggests how to describe an architecture in a way that its properties, such as fault tolerance, can be explored.

Software redundancy does not necessarily increase fault tolerance. If the redundant software units contain the same code, then the conditions that cause one unit to fail are likely to cause other copies of the same software to fail. Software redundancy requires independent development of the parallel software units.

For some applications, fault tolerance may be achieved by manipulating the input data so that all software units are processing slightly different data — although not so different as to affect the outcome. Thus data that causes one software unit to fail might (after manipulation) not cause a parallel unit to fail.

D.3.3 Computing Platforms

The computing platform consists of the hardware and operating system on which the application software will run. A software qualification effort should consider the specific configuration of hardware and operating system to be used.

Computers may be based on general purpose processors (e.g., Intel) or specialized processors (e.g., video, programmable logical controllers). Turnover in special purpose processors is frequent, so the technology qualification effort should consider the likelihood of the continued availability of specialized processors during the intended life of the system.

The two most common operating systems are Microsoft Windows and Linux (open source). Windows is commonly used on general purpose processors, while Linux is commonly used on specialized processors such as communications servers.

Software may operate in a network environment where other devices such as sensors, routers, multiplexers, data stores, and printers are connected. OPC specifications provide guidance on interfacing devices in such a network.


D.3.4 Programming Languages

The software industry has developed a wide variety of programming languages, often for very specific applications. The appropriateness of the selected programming language for the intended application should be considered in the Software technology Qualification effort. Some examples of typical considerations follow.

Programmers write source code statements. A compiler converts these into object code that is loaded onto the computer and executed. Interpreted languages are not compiled. The actual source statements are directly executed by the interpreter. Interpreted languages tend to be simple. Such programs are easy to change. However, they tend to be inefficient in terms of memory use and execution speed.

Some languages are strongly typed. This means that the programmer must explicitly define each variable before it can be used. This requirement prevents many common programming errors such as creating a new variable through misspelling and corrupting a variable by loading the wrong type of data (e.g., writing an alphabetic character into a numeric variable).

Compilers vary in terms of the quality and efficiency of the object code they produce. Compilers may introduce defects in the course of processing source code. This is most common with compilers developed for new languages or converted to support new hardware.
Maturity of the language and compiler is an important consideration in software technology qualification. Suppliers of programming languages may eventually stop supporting a language or a specific version of it. This means that, at some point, language features may fail and the software will cease to operate correctly, if at all.

D.3.5 COTS and Legacy Software

Large software systems usually take advantage of previously developed code. This may be legacy (developed by the technology supplier) or Commercial off the Shelf (COTS) purchased from an external source (e.g., MATLAB). If the COTS or Legacy software are mature and being used without change, then they may be excluded from the qualification effort. If they are being modified for a new application, or if they are not mature, then they should be evaluated as part of the qualification effort. Obtaining design information and source code for COTS and legacy software may be difficult. If these are not available, the qualification effort will depend on information obtained from testing and prior use of the software.

D.3.6 Security

Information security is an increasing concern for software-intensive systems. Traditionally, isolated systems such as rigs, platforms, and ships relied on physical security of the computers to prevent malicious access. However, as suppliers move towards remote diagnostic and repair across the internet, physical security is no longer adequate. Software protections such as firewalls and virus detectors should be considered. Also, programming practices employed in application and operating system software can be improved to minimize the potential for break-ins. ISO/IEC 27002 identifies many practices important to maintaining information security.

D.3.7 Reliability Analysis

Typically, reliability analysis is concerned with predicting the Mean-Time-to-Failure (MTTF) or Probability of Failure on Demand (PFD) of a system. This can be used with other information, such as the time required to implement fixes, to estimate the availability of a system. Usually, MTTF of PFD is most important for safety critical systems. Availability may be more important for business critical systems. The Technology Specification should define which notions of reliability are most important for the system undergoing qualification.

- MTTF Mean-time-to-Failure
- PFD Probability of Failure on Demand
- Latent Defects
- Future Backlog
- Availability.

As noted previously, software does not wear out – the causes of its failure are implemented in the code. Thus, software reliability analysis usually includes predicting the number of latent (undetected) defects present in the software. Once defects have been detected, users will continue to encounter them until they are fixed. Estimating and managing the backlog of defects also are important in managing system availability, as most software systems require continuing maintenance.

Reliability modelling typically involves curve fitting. Data from early verification and validation activities are used to estimate the parameters of a model that then is used to predict future performance in terms of MTTF or defect discovery. The logarithmic Poisson and Weibull distributions are widely used for software reliability analysis.

Several factors contribute to the tendency of software failure data (collected across the life cycle) to take on a Weibull distribution. The Weibull model assumes defect insertion and detection are proportional to developer and tester effort. Project staffing tends to increase early in the project, stay constant, then falls off at the end. Insertion of defects tends to occur early in the life cycle, while detection of defects tends to be concentrated in later activities. Fixing defects tends to introduce new defects. The Weibull distribution is characterized by three parameters: shape, location of centre, and scale. The scale factor corresponds to the total number of defects present. Thus fitting early data to the Weibull distribution produces an estimate of the total number of defects to be found. This can be compared with the actual number found during testing to assess the reliability of the delivered software.

When only failure data from testing at the end of the life-cycle is considered, that data is more likely to follow the form of a logarithmic Poisson distribution where the failure rate decreases monotonically. When testing occurs throughout the life-cycle, as in incremental or agile development, the Weibull model may be more appropriate.

API RP 17N describes a detailed process (Annex B) and several specific methods for reliability analysis (Annex C and D). Most of the discussion focuses on hardware reliability, but some of the same mathematical models apply to software. IEEE 1061 discusses several software reliability models.
D.4 Examples of Software Reliability Analysis

Figure D-2 shows an example where data on the number of defects found through Week 30 of testing was used to estimate the parameters of a Weibull distribution through Week 85. The scope parameter (area under the curve) indicated that 5000 defects can be expected. During Week 30 through 45, actual results continue to exceed the Weibull prediction, suggesting that the model parameters may need to be re-estimated and that the number of defects exceeds 5000.

If data on detect rates (defects per unit of testing, e.g., effort hours) is available, then some variation of the logarithmic Poisson model may be a better choice. Figure D-3 shows a simple logarithmic Poisson model fitted to data on defects per staff-day of effort. Reliability can be read from the chart as the inverse of defect rate. The graph can be used to predict how much additional testing is necessary to reach a desired reliability level.
APPENDIX E  USE OF HISTORICAL RELIABILITY DATA

E.1 Evaluation of the quality of the databases

E.1.1 Introduction
The purpose of this Appendix is to provide guidance on the use of historical reliability data when that is needed for technology qualification.

Extracting and applying historical reliability data is not straightforward even when the data is relevant and the technology has already been qualified or is proven. The Offshore Reliability Database (OREDA) is commonly used in the offshore industry as the source for historical data. This can be satisfactory for offshore equipment. But it is important to identify all available data and not exclude data without evaluation. Besides dedicated databases, relevant data can be found in proceedings from conferences or in technical articles in periodicals.

When evaluating the quality of reliability data, there are three important elements that should be considered:

1) the quality of the data available in the database (Evidence and Argument.)
2) the quality of the database, i.e. the structure and set-up (Argument.)
3) the relevance of the data in the database. (Context and Claim.)

E.1.2 Quality of data
The data quality depends on many factors related to the data collection process. It is difficult for the analyst to evaluate the quality of the data collection process because the necessary information would not be available. The best option may be to evaluate data quality based on general sources such as quality and verification reports for the data collection process.

E.1.3 Quality of the database
The quality of the database is related to its consistency. Important aspects are whether:

— There is an unambiguous and efficient coding system.
— Qualified people are responsible for the recording, storing and quality control of the data.

More details on best practices and recommendations for quality databases can be found in ISO 14224. Some vital information that normally must be available for the database to get a high score / high rating according to ISO 14224, includes:

— System boundaries must be defined. For instance if a pump is driven by an electric motor, we must know if motor failures are included in the pump failures, or if they are found somewhere else in the database.
— Failure modes must be defined and not overlapping.
— The number of failures and the operating and calendar time must be given.
— It must be stated if repair time means active repair time.

Some additional information that will contribute to a high score is:

— Description of system characteristics, like design parameters.
— Description of operational conditions.
— Description of preventive maintenance.
— Description of environmental conditions.

E.1.4 Relevance of the data
The relevance of the data depends on factors such as:

— To what extent the failure data from a valve in a nuclear power station is representative for a valve on an offshore installation.
— To what extent failure data from a compressor operated since 1980 are representative for a new compressor.
— To what extent failure data from one offshore platform are representative for another.
— To what extent failure data from valves in general are representative for ball valves.

The purpose of such questions is to help the analyst in selecting and evaluating the databases. It is important to recognize that the relevance of the database depends on the intended use of the data. If the purpose of the reliability analysis is to determine the optimal number of different types of spare parts, the analyst needs equipment information down to the spare part level. If the purpose is to give an overall estimate of system performance, this may not necessarily be required.

The final evaluation of the reliability data sources depends on the intended use of the data. The information that is relevant and sufficient for one analysis may not fit for a more detailed analysis.
E.2 Example of extracting Data from a Database

The table below shows some figures for gas turbines from the OREDA 2002 handbook and is a good illustration of the challenges the analyst faces when using typical databases. The estimator for the failure rate is the number of critical failures divided by the total operating time.

<table>
<thead>
<tr>
<th>OREDA taxonomy</th>
<th>Equipment Description</th>
<th>Failure rate per 10^6 hours</th>
<th>Number of failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2</td>
<td>Gas turbines</td>
<td>527.59</td>
<td>941</td>
</tr>
<tr>
<td>1.2.1</td>
<td>Aero derivative</td>
<td>684.18</td>
<td>604</td>
</tr>
<tr>
<td>1.2.1.1</td>
<td>- 1000 kW</td>
<td>366.63</td>
<td>57</td>
</tr>
<tr>
<td>1.2.1.2</td>
<td>3000 – 10000 kW</td>
<td>279.08</td>
<td>20</td>
</tr>
<tr>
<td>1.2.1.3</td>
<td>10000 – 20000 kW</td>
<td>1079.79</td>
<td>176</td>
</tr>
<tr>
<td>1.2.1.4</td>
<td>20000 – 40000 kW</td>
<td>868.45</td>
<td>296</td>
</tr>
<tr>
<td>1.2.1.5</td>
<td>Unknown</td>
<td>362.23</td>
<td>55</td>
</tr>
<tr>
<td>1.2.2</td>
<td>Industrial</td>
<td>374.12</td>
<td>337</td>
</tr>
<tr>
<td>1.2.2.1</td>
<td>- 1000 kW</td>
<td>199.73</td>
<td>13</td>
</tr>
<tr>
<td>1.2.2.2</td>
<td>1000 – 3000 kW</td>
<td>613.32</td>
<td>21</td>
</tr>
<tr>
<td>1.2.2.3</td>
<td>3000 – 10000 kW</td>
<td>260.67</td>
<td>128</td>
</tr>
<tr>
<td>1.2.2.4</td>
<td>10000 – 20000 kW</td>
<td>410.14</td>
<td>87</td>
</tr>
<tr>
<td>1.2.2.5</td>
<td>20000 – 40000 kW</td>
<td>895.30</td>
<td>88</td>
</tr>
</tbody>
</table>

Assuming that an analyst performs a production availability study of a system where one component is a gas turbine, Aero derivative, 15000 kW. Some obvious candidates for the failure rate are:

- Gas turbines (1.2) 527.59
- Aero derivative (1.2.1) 648.18
- 10000-20000 kW (1.2.1.3) 1079.79
- Combination (1.2.1.3 + 1.2.2.4) 858.27.

The reliability data differs significantly depending on the specific dataset selected. An important observation about the data is that all groups have a significant number of failures. The statistical background for all these predictions should therefore be reasonably good. There is therefore little support directly from the database as to which data-set should be selected. The recommended solution is therefore to present the data to a group of experts for a systematic expert judgement and evaluation of what data would be the most relevant to use when evaluating the specific gas turbine in question.
APPENDIX F INTRODUCTION TO SYSTEMS-ENGINEERING APPROACHES

F.1 Introduction

The main advantages of a systems engineering-approach to technology qualification are to:

1) Allow representing the reasoning used to prove achievement of goals explicitly based on the evidence provided.
2) Allow this reasoning to be challenged and refined as experience with and evidence about the technology is obtained.
3) Provide a framework for eliciting expert judgments that, as far as possible, avoids biases.
4) Provide a means to assess the impact of estimated uncertainties on the probability of reaching the overall goal.
5) Provide a means to assess the required reduction of uncertainties in order to obtain an acceptable probability of reaching the overall goal.
6) Develop confidence from the above-mentioned reasoning throughout the Technology Qualification Process.

Systems engineering is an interdisciplinary approach to ensure that important information is secured and maintained throughout the lifecycle of the system. This requires a methodology that brings clarity and enables transparency between all engineering disciplines involved.

The systems engineering approach to technology qualification aims to satisfy the goals and functional requirements specified in the Technology Qualification Basis. These typically address:

— Reliability: continuity of correct service.
— Availability: readiness for correct service.
— Maintainability: ability to undergo modifications and repairs.
— Safety: absence of catastrophic consequences on the user(s) and the environment.
— Integrity: absence of improper system alterations.

As such, this is closely related to the normal dependability analyses commonly used in software development. Dependability is defined as the ability to avoid service failures that are more frequent and more severe than is acceptable and is a function of the parameters listed above.

The systems engineering approach to TQ aims to provide the stakeholders with an explicit body of evidence forming a convincing and valid argument that the technology fulfils the specified goals and functional requirements for a given application in a given environment. The basic anatomy of the argument is shown in Figure E-1.

![Figure F-1](image-url)

The basic anatomy of the argument expressed in a goal model
F.2 A model based approach

Models can help to better understand the argumentation supporting the technology qualification. Models achieve this by better communicating the understanding and intent (to others and to oneself) than the traditional documents-based approach. The model-based approach relies on the following four cornerstones.

— Goal modelling that explicitly represents the reasoning from lower-level goals to the satisfaction of the overall goal.
— Linking evidence to lowest-level goals; the leaf goals.
— Elicitation from experts of how well available evidence fulfils leaf goals.
— Propagation of goal fulfilment and uncertainty to overall goals.

F.3 Goal modelling

The hierarchical structure of the goal decomposition can be captured in a goal model. The goal model captures the argumentation for the dependability case by graphically showing how the goals are broken down into sub-goals. Goals can be broken down along different dimensions. Functional, structural and process dimensions are the most commonly used. There would normally be a mix of functional and structural decomposition in the goal model. Another feature in goal models is the notion of obstacles that can represent failure modes preventing a goal from being satisfied. This enables formulating fulfilment of goals in terms of failure modes and associated failure mechanisms. In this way, goal modelling can support conducting and recording of results from FMEA and FTA sessions. There are different notations for goal models with different expressive power and semantics. GSN, I* and KAOS are the most common of them. An example is shown below with the KAOS notation.

F.4 Linking evidence to leaf goals

The decomposition of goals ends when the sub-goals are fine-grained enough to enable collecting direct evidence about their satisfaction. These lowest level sub-goals are the leaf goals. These leaf goals are connected to evidence, typically produced in verification and validation activities such as testing, analyses, inspections etc.

![Goal Model Diagram](image)

Figure F-2
Illustration of the principle of goal modeling, showing the KAOS notation
F.5 Systematic elicitation of expert opinions of how well available evidence fulfils leaf goals

The assessment of how well the evidence provided fulfil the specified goals necessarily depends on subjective judgment by experts. Hence, it is essential to take measures to ensure that these judgments are elicited as precisely as possible. Established principles for expert elicitation help eliminate systematic errors (i.e. bias). In this process, the expert is asked to provide a quantitative measure indicating how well the provided evidence fulfils the leaf-goal. This measure covers a range indicating the degree of uncertainty of the expert about whether the evidence really fulfils the leaf goal.

At intermediate steps of the basic qualification process, when qualification activities have not been completed and hence some of the evidence that is planned to be provided in support of the qualification is missing, one may choose to include expert opinions regarding

— the probability that the planned activities will actually succeed in providing the evidence required
— the probability that this can be achieved within the schedule and budgets assigned to these unfinished activities.

In this way, the goal model can support assessment and management of qualification risks.

F.6 Propagation of goal fulfilment and uncertainty to overall goals

When all leaf-goals are assessed, the values and uncertainty ranges elicited from the experts can be propagated upwards in the goal model. This can be achieved by the use of Monte Carlo simulation. The results from the propagation are uncertainty distributions of the parent goals up to the main goal.
CHANGES – HISTORIC

Note that historic changes older than the editions shown below have not been included. Older historic changes to this document (if any) may be obtained through http://www.dnv.com.

December 2012 edition

Main changes

Since this Recommended Practice was published as a main revision in July 2011, text and figures have been updated for consistency.