

Recommended Practice for Subsea Production System Reliability and Technical Risk Management

API RECOMMENDED PRACTICE 17N
FIRST EDITION, MARCH 2009



Recommended Practice for Subsea Production System Reliability and Technical Risk Management

Upstream Segment

API RECOMMENDED PRACTICE 17N
FIRST EDITION, MARCH 2009



Special Notes

API publications necessarily address problems of a general nature. With respect to particular circumstances, local, state, and federal laws and regulations should be reviewed.

Neither API nor any of API's employees, subcontractors, consultants, committees, or other assignees make any warranty or representation, either express or implied, with respect to the accuracy, completeness, or usefulness of the information contained herein, or assume any liability or responsibility for any use, or the results of such use, of any information or process disclosed in this publication. Neither API nor any of API's employees, subcontractors, consultants, or other assignees represent that use of this publication would not infringe upon privately owned rights.

Classified areas may vary depending on the location, conditions, equipment, and substances involved in any given situation. Users of this recommended practice should consult with the appropriate authorities having jurisdiction.

Users of this recommended practice should not rely exclusively on the information contained in this document. Sound business, scientific, engineering, and safety judgment should be used in employing the information contained herein.

API publications may be used by anyone desiring to do so. Every effort has been made by the Institute to assure the accuracy and reliability of the data contained in them; however, the Institute makes no representation, warranty, or guarantee in connection with this publication and hereby expressly disclaims any liability or responsibility for loss or damage resulting from its use or for the violation of any authorities having jurisdiction with which this publication may conflict.

API publications are published to facilitate the broad availability of proven, sound engineering and operating practices. These publications are not intended to obviate the need for applying sound engineering judgment regarding when and where these publications should be utilized. The formulation and publication of API publications is not intended in any way to inhibit anyone from using any other practices.

Any manufacturer marking equipment or materials in conformance with the marking requirements of an API standard is solely responsible for complying with all the applicable requirements of that standard. API does not represent, warrant, or guarantee that such products do in fact conform to the applicable API standard.

All rights reserved. No part of this work may be reproduced, translated, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission from the publisher. Contact the Publisher, API Publishing Services, 1220 L Street, N.W., Washington, D.C. 20005.

Copyright © 2009 American Petroleum Institute

Foreword

Nothing contained in any API publication is to be construed as granting any right, by implication or otherwise, for the manufacture, sale, or use of any method, apparatus, or product covered by letters patent. Neither should anything contained in the publication be construed as insuring anyone against liability for infringement of letters patent.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the specification.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the specification.

This document was produced under API standardization procedures that ensure appropriate notification and participation in the developmental process and is designated as an API standard. Questions concerning the interpretation of the content of this publication or comments and questions concerning the procedures under which this publication was developed should be directed in writing to the Director of Standards, American Petroleum Institute, 1220 L Street, N.W., Washington, D.C. 20005. Requests for permission to reproduce or translate all or any part of the material published herein should also be addressed to the director.

Generally, API standards are reviewed and revised, reaffirmed, or withdrawn at least every five years. A one-time extension of up to two years may be added to this review cycle. Status of the publication can be ascertained from the API Standards Department, telephone (202) 682-8000. A catalog of API publications and materials is published annually by API, 1220 L Street, N.W., Washington, D.C. 20005.

Suggested revisions are invited and should be submitted to the Standards Department, API, 1220 L Street, NW, Washington, D.C. 20005, standards@api.org.

Copyright American Petroleum Institute
Provided by IHS under license with API
No reproduction or networking permitted without license from IHS

Contents

	Page
1 Scope	1
1.1 Project Types	2
1.2 Equipment Types	2
1.3 Project Stages	2
1.4 Qualification	3
2 Other Related Documents	3
2.1 API Specification Q1 (ISO/TS 29001)	3
2.2 DNV RP A203 and API Recommended Practice 17Q	3
2.3 ISO 20815	3
3 Terms and Definitions	4
4 Abbreviations	6
5 Overview of Reliability and Technical Risk Management	7
5.1 Underlying Structure	7
5.2 Define	9
5.3 Plan	10
5.4 Implementing the Plan	10
5.5 Feedback	11
5.6 Supporting Reliability Key Processes (KPs)	12
5.7 Summary	13
6 Recommended Practice for Each Project Stage	13
6.1 General	13
6.2 Technical Risk and Reliability Effort	13
6.3 Feasibility Stage	15
6.4 Concept Selection	17
6.5 Front End Engineering Design (FEED)	19
6.6 Detail Design and Manufacture	21
6.7 System Integration Test (SIT), Install, Commission and Operate	24
Annex A (informative) Technical Risk Categorization Approach to Reliability and Technical Risk Management	26
Annex B (informative) Detailed Reliability Process and Activity Description	39
Annex C (informative) Reliability Data Management	89
Annex D (informative) Application of Test Statistics	94
Figures	
1 Define, Plan, Implement and Feedback Loop	8
2 Project Life Cycle	14
3 Key Process (KP) Interaction with Define, Plan, Implement, and Feedback Loop	15
4 Guide to Process Effort by Project Phase and Risk	16
B.1 Procedure for Defining Availability Goals and Requirements	42
B.2 Functional Test Logic	74
B.3 Outline Qualification Process	77
B.4 Example Output from Reliability Capability Maturity Assessment	82
C.1 Data Collection and Usage Strategy	91

Tables

A.1	Technical Risk Categorization	27
B.1	Availability Performance Metrics Example.	42
B.2	Value Metrics Examples	44
B.3	Primary Drivers and Influences for Planning for Availability	47
B.4	Guidance on the Level of Effort Required for Reliability Effort	48
B.5	Types of Reliability Assurance Evidence	54
B.6	Suggested Constituent Parts of a Reliability Assurance Document (RAD)	55
B.7	Relationship of Analysis Type to Project Stage and Technical Risk Categorization.	57
B.8	Failure Modes, Effects and Criticality Analysis (FMECA) Summary	58
B.9	Fault Tree Analysis (FTA) Summary	59
B.10	Reliability Block Diagram (RBD) Summary	60
B.11	Event Tree Analysis (ETA) Summary	61
B.12	Physics of Failure Summary	62
B.13	Importance Analysis Summary	63
B.14	Qualitative Common Cause Failure Analysis Summary	64
B.15	Quantitative Common Cause Failure Analysis Summary	65
B.16	Reliability Availability Maintainability (RAM) Analysis Summary	66
B.17	Root Cause Analysis (RCA) Summary	67
B.18	Recommended Verification and Validation of the Key Processes (KPs)	68
B.19	Definition of Technology Readiness Levels (TRLs)	75
B.20	Standard Reference for Goodness of Fit Test	76
B.21	Standard Reference for Reliability Parameter Estimates	78
B.22	Standard Reference for Compliance Tests	78
B.23	Standard Reference for Comparison Test	78
B.24	Overview of Reliability Capability Maturity Levels	81
B.25	Some Instruments for Learning	86
D.1	Example of Sorted Failure Data	94
D.2	Example T_i Values	95

Introduction

Poor reliability can have a major financial impact for all organizations involved in designing, manufacturing, installing and operating subsea equipment. The complexity of technical and organizational challenges in subsea projects requires continual attention to detail to achieve high reliability performance.

Budget and schedule constraints usually imply limited information and time for making decisions. This tends to introduce varying levels of uncertainty which have the potential to affect equipment reliability.

This recommended practice provides a structured approach which organizations can adopt to manage this uncertainty throughout the life of a project. This may range from the management of general project risk through to the identification and removal of potential failure modes in particular equipment.

Most organizations will find much that is familiar and recognized as good practice. Some sections of the annex may only be of interest to the reliability specialist. The basic approach however, is simple and consistent and when applied correctly has the potential to greatly reduce the financial risk of designing, manufacturing, installing and operating subsea equipment.

Copyright American Petroleum Institute
Provided by IHS under license with API
No reproduction or networking permitted without license from IHS

Recommended Practice for Subsea Production System Reliability and Technical Risk Management

1 Scope

The application of subsea technology in the offshore oil and gas industry demands large capital investments and significant operational expenditures. The value of using subsea technology depends on its production availability (see 3.17) which is a reflection of its reliability and maintainability (RM).

This API recommended practice (RP) aims to provide operators, contractors and suppliers with guidance in the application of reliability techniques to subsea projects within their scope of work and supply only. It is applicable to:

- standard and non-standard equipment,
- all phases of projects from feasibility studies to operation.

This RP does **not** prescribe the use of any specific equipment or limit the use of any existing installed equipment or indeed recommend any action, beyond good engineering practice, where current reliability is judged to be acceptable. It is also **not** intended to replace individual company processes, procedures, document nomenclature or numbering; it is a guide. However, this RP may be used to enhance existing processes, if deemed appropriate.

Users of this RP should gain a better understanding of how to manage an appropriate level of reliability throughout the life cycle of their subsea projects. Industry wide, users should be able to:

- recognize the trade off between up front reliability and engineering effort vs. operational maintenance effort,
- provide better assurance of future performance of subsea systems,
- effectively manage the risks from using novel equipment and standard equipment in novel applications,
- schedule projects with sufficient time to address all the technical risks.

Overall, this should lead to better understanding of technical risk and, therefore, greater confidence in economically or technically challenging developments.

Furthermore, this RP provides the industry with a common framework and language, compatible with ISO 20815, *Petroleum, petrochemical and natural gas industries—Production assurance and reliability management*, for the specification and demonstration of reliability achievement between operators, contractors, and suppliers.

Reliability is a topic which is best addressed through industry wide cooperation in terms of best practice, managing failures that do occur and the collection and analysis of performance data. This RP aims to provide a starting point for developing common understanding and cooperative progress within the subsea oil and gas industry.

The achievement of improved subsea equipment availability requires good engineering and management processes, practices and behaviors at an organizational level to manage and minimize the potential for equipment failure.

The focus of this RP however, is on specific activities (or tasks) that can be implemented within projects to achieve immediate and tangible improvements to system performance.

1.1 Project Types

The RP is provided as a guide to the whole of the subsea industry and is intended to be applicable to all project scopes including:

- repeat field development projects using field proven or fully qualified hardware,
- new technology development projects,
- field development projects in which existing technology is used under extended operating conditions,
- field development projects involving new technology.

The philosophy of this RP is to prioritize reliability and technical risk management efforts based on the level and source of technical risk in the project. More detailed reliability effort is recommended for projects/equipment involving high technical risk.

For projects/equipment involving low technical risk (e.g. some projects using field proven or fully qualified hardware), little reliability effort beyond existing good engineering and management practices is expected.

1.2 Equipment Types

The RP applies to all subsea equipment including the following.

- **Subsea Equipment and Hardware**

From the sand face downhole to the top of the riser as defined in API 17A. This would normally also include: downhole and completion components; well systems; topside interfaces; controls; flowlines; pipelines.

- **Installation Facilities and Tools**

Risks associated with installation facilities, equipment, tools and procedures should be included to ensure that the construction procedures will not adversely affect the reliability of permanently installed equipment.

- **System Interfaces**

Risks posed by hardware interfaces should be addressed, particularly when these interfaces also represent boundaries between different organizations in the supply chain or teams within the project management organization.

- **Subsea Intervention and Maintenance**

Workover and intervention methods and tools should be included in the subsea system assessment where these have a direct bearing on subsea system maintainability and availability.

1.3 Project Stages

This RP covers all stages of a subsea project from feasibility through design to operation as follows:

- feasibility;
- concept selection;
- front end engineering design (FEED);
- detail design and manufacture;
- system integration test (SIT), installation, commissioning and operations.

1.4 Qualification

Qualification is the process of independently confirming by examination, testing or some other defining evidence, that equipment meets specified requirements for the intended use. The risk of equipment *not* being fit for purpose or determined as *unqualified*, is specifically addressed at each project stage within the RP. Users of this specification may have their own processes for qualifying equipment, in which case many of the qualification tasks recommended here may be unnecessary.

For projects involving fully qualified equipment and low additional risk, the demands of this RP should be minimal. However, as technical risk is a broad topic, it may not be entirely addressed through a program of qualification testing alone. Even equipment believed to be fully qualified should be considered in terms of broader technical risks in line with this RP to verify that all have been addressed.

2 Other Related Documents

2.1 API Specification Q1 (ISO/TS 29001)

API Q1 (ISO/TS 29001) is a fundamental standard used by the subsea oil and gas industry for the achievement of quality in products and services. This RP has been developed to be consistent with the requirements of API Q1.

Reliability achievement demands attention to quality in design and manufacture as reliability in design will not be realized if the required quality is not delivered. However, high quality cannot improve the inherent reliability of an unreliable design. Therefore, this RP includes good practices for reliability management (e.g. the setting of goals and requirement, the implementation of system RAM analyses, reliability testing, etc.) which are not generally included in conventional quality assurance (QA) and quality control programs.

2.2 DNV RP A203 and API Recommended Practice 17Q

DNV RP A203 and API 17Q recommend that the identification of technical risk and in particular equipment failure modes be used as the basis for determining equipment qualification status. This is comparable with the method of 'reliability' categorization of new technology based on the concept of TRL as described in B.6.

The qualification of new technology for use within subsea projects is a topic closely related to reliability and is identified as a key reliability process (see B.6).

2.3 ISO 20815

ISO 20815 addresses production assurance and reliability management in the petroleum, petrochemical and natural gas industries. ISO 20815 requires a production assurance program (PAP), which encompasses the definition, planning and updating of RM activities to be performed during the life cycle of a project or assets already operating.

This RP is intended as a guide on how to implement ISO 20815 within subsea projects. Projects implemented in compliance with this RP shall be considered compliant with ISO 20815.

The six key aspects of the PAP defined in ISO 20815 have been used as the basis for the reliability and technical risk management program defined in this RP.

Projects implemented in compliance with ISO 20815 may be considered compliant with this RP. However, the lower level of detail in ISO 20815 may result in the omission of some API recommended activities in this RP.

3 Terms and Definitions

For the purposes of this document, the following definitions apply.

3.1

availability

The ability of an item to be in a state to perform a required function under given conditions at a given instant of time, or in average over a given time interval, assuming that the required external resources are provided.

NOTE High availability can be achieved through high reliability (equipment rarely breaks down) or maintainability (when equipment breaks down it is repaired quickly) or a combination of both.

3.2

availability requirements

Appropriate combination of reliability and/or maintainability performance characteristics that need to be achieved to meet project requirements.

3.3

common cause failure

Failures of different items resulting from the same direct cause, occurring within a relatively short time, where these failures are not consequences of another.

NOTE Components that fail due to a shared cause normally fail in the same functional mode. The term common mode is, therefore, sometimes used. It is, however, not considered to be a precise term for communicating the characteristics that describe a common-cause failure.

3.4

down time

The time interval during which an item is unable to perform a required function due to a fault, or other activities (e.g. during maintenance).

3.5

failure

Termination of the ability of an item to perform a required function.

NOTE 1 After failure, the item has a fault.

NOTE 2 "Failure" is an event, as distinguished from "fault," which is a state.

3.6

failure data

Information related to the occurrence of a failure event.

3.7

failure impact (effect)

Consequence of a failure on a system, on an equipment function, on the economy, on human safety or on the environment.

3.8

failure mechanism

A process (physical, chemical, human, or other) that leads to a failure.

NOTE Most failure mechanisms involve more than one process and occur as a chain of events and processes.

3.9**failure mode**

The effect by which a failure is observed on the failed item [i.e. the loss of a required functionality (e.g. loss of containment)].

3.10**fault**

State of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources.

NOTE A fault is often a result of a failure of the item itself but the state can exist without a failure.

3.11**installation hardware**

The system or equipment used to install subsea production hardware.

3.12**maintainability**

Ability of an item under given conditions of use, to be retained in, or restored to, a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources.

3.13**maintenance free operating period****MFOP**

The time that a system can operate without a specified failure event that demands a maintenance intervention, where the failure occurrence is to a given level of probability.

3.14**maintenance record**

Set of data that contains all failure, fault, and maintenance information relating to an item.

3.15**package**

A named system, subsystem, or defined set of components considered as a single entity for the purposes of a design study or for procurement (e.g. subsea tree, control system).

3.16**process**

An arrangement of tasks directed towards a specific objective.

3.17**production availability**

The ratio of actual production to a reference (e.g. planned) production level over a specified period of time.

3.18**qualification**

The process of confirming, by examination and provision of evidence, that equipment meets specified requirements for the intended use.

3.19**redundancy**

Existence of more than one means to perform a required function (e.g. by duplicating items).

3.20**reliability**

The ability of an item to perform a required function, under given conditions of production, environment, and usage, for a required time interval.

3.21**risk**

The potential for the realization of unwanted, negative consequences of an event. Risk can be measured by the product of the probability of the event occurrence and the consequence of the event.

3.22**reliability and maintainability data****RM data**

Data collected to support analysis of reliability, maintainability and availability.

NOTE RM data is the term applied by ISO 14224. ISO 20815 refers to reliability data instead.

3.23**specification**

The document in which functional, performance, design and operating requirements are defined.

3.24**system availability**

The ratio of time a system or component is functional or in a functional state to the total time it is required or expected to function.

3.25**uncertainty**

A state of having limited knowledge where it is impossible to exactly describe the existing state or future outcome(s).

3.26**uptime**

The time interval during which an item is functional.

3.27**validation**

The process that substantiates whether technical data and engineering models are within the required range of accuracy, consistent with the intended application.

3.28**verification**

The process that determines the extent to which a procedure, task, physical product, or model conforms to its specification.

4 Abbreviations

CAPEX	capital expenditure
CHR	constant hazard rate
ESS	environmental stress screening
ETA	event tree analysis
FAT	factory acceptance test
FEED	front end engineering design

FMECA	failure modes, effects and criticality analysis
FTA	fault tree analysis
GOR	gas-to-oil ratio
HALT	highly accelerated life test
HASS	highly accelerated stress screening
HAZOPS	hazards and operability study
IRR	internal rate of return
KP	key process
LCC	life cycle cost
MCS	Monte Carlo simulation
MFOP	maintenance free operating period
MTBF	mean time between failure
NPV	net present value
OPEX	operating expenditure
OREDA	offshore reliability data
PAP	production assurance program
PARLOC	pipeline and riser loss of containment
PFMEA	process failure modes and effects analysis
QA	quality assurance
RAD	reliability assurance document
RAM	reliability, availability and maintainability
RBD	reliability block diagram
RBDA	reliability block diagram analysis
RCA	root cause analysis
R&D	research and development
RM	reliability and maintainability
ROV	remotely operated vehicle
RP	recommended practice
SIT	system integration test
TRL	technology readiness level

5 Overview of Reliability and Technical Risk Management

This section summarizes the basic philosophy behind this RP. It explains the key sequence of “*Define, Plan, Implement and Feedback*” that is the basis behind all of the reliability activities described later.

5.1 Underlying Structure

This RP is based on the same twelve “key” reliability processes as defined by ISO 20815 for production assurance and reliability management, listed in 5.6 and described in detail in Annex B. These processes, if adopted, provide an organization with an overall good capability in management of reliability.

However, the focus of this RP is project execution, which is more practically described as a number of integrated reliability and technical risk management activities [which are derived from the key processes (KPs)].

These activities have been arranged into a cycle of four basic steps as illustrated in Figure 1. These are applied during each project stage and also for each piece of reliability work. The cycle encourages a “stop and think” approach to ensure:

- clear objectives are set for the work;
- appropriate activities are selected that will meet the objectives;
- there is sufficient time and resource to carry out the activities;
- there is confirmation that the activities have been completed correctly;
- lessons are learned to improve the next project.

Much of this is good organizational practice, but in addition, the reliability and risk management focus is on removing potential causes of poor reliability at every step.

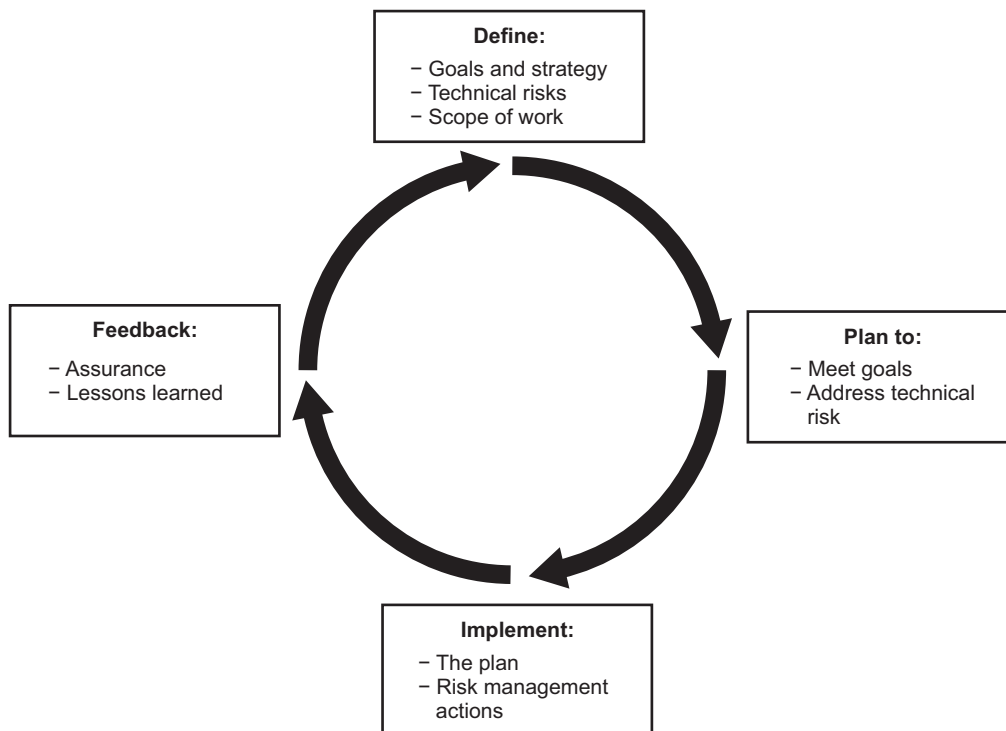


Figure 1—Define, Plan, Implement and Feedback Loop

As the project progresses through the various project stages, the focus of the reliability and technical risk management program, as defined in the above *Define, Plan, Implement and Feedback* loop, will change as the subsea system becomes better defined. This RP suggests adopting the following approach to the different project stages.

- **Feasibility—project level view** considers the overall system challenges to project performance (location, environment, new technology).
- **Concept selection—system level view** considers the reliability implications of technology and different possible system configurations.

- **FEED—package level view** considers what requirements need to be specified on individual packages to meet overall system goals (e.g. well, manifold, umbilicals).
- **Detail design and manufacture—subassembly and component level view** considers the reliability risks associated with individual components (e.g. gate valves, connectors, sensors).
- **SIT, install, commission and operate—procedural level view** considers how procedural control can be used to prevent errors which can affect reliability performance after manufacture. This also includes measuring and maintaining actual performance and collecting information to improve future projects.

5.2 Define

The initial step is to identify the project's reliability goals and prioritize reliability and technical risk management effort within the project. This should include the following activities.

5.2.1 Goals, Strategy and Requirements

It is important for the project to be clear on what it is aiming to achieve and why. This can be defined as:

- the reliability performance that the project **would like to achieve (goals)**, and/or
- the reliability performance that the project **must achieve** in order to meet the business objectives of the project (**requirements**).

Goals and requirements may be expressed in words (qualitative) or numerically (quantitative).

The **strategy** is the general approach the project will take to deliver the stated goals and requirements in a way that adds value for the project. For example, the strategy may be to:

- extend the life of equipment before failure (**reliability strategy**);
- minimize the time to restore failed equipment to an operable state (**maintainability strategy**);
- use operational mitigations, such as spare capacity, to reduce the effect of system failure (**risk mitigation strategy**).

This RP recommends implementing a reliability and technical risk management program which combines all of the above, although the focus is on managing risks through improved design and manufacture.

5.2.2 Assessment of Technical Risk

The risk assessment effort should be tailored to the level and source of technical risk in the project and the project stage being considered.

The assessment of technical risk will take different forms during different stages of the project, for example:

- a simple high level technical review may filter out equipment with technical uncertainty;
- consequence/severity analysis can be used to identify equipment with the greatest impact on production or safety and environment;
- identification of potential failure modes (or risk of failure) (e.g. by FMECA);
- technical risk reviews can be used to identify where equipment is being designed beyond current experience.

The assessment of technical risk should seek to identify “change” factors which introduce uncertainty to the ability of the equipment to operate reliably in the field.

5.2.3 Identification of Scope of Work

The scope of work for any given project stage is the list of activities which will address the identified technical risks. This will usually include activities such as:

- system availability analysis to confirm that design configurations meet economic targets;
- FMECA to identify, address and if possible, design out potential failure modes;
- design reviews to expose designs at various stages to expert opinion;
- testing and analysis to develop understanding of and demonstrate potential for functionality and reliability.

All activities should:

- add value to the project,
- be consistent with the project goals and strategy.

5.3 Plan

The plan establishes the detail of how the reliability scope of work is to be accomplished.

The reliability and technical risk management plan for each project stage will cover areas such as:

- resources (people, software/hardware, etc.);
- roles and responsibilities;
- deliverables for each activity;
- schedules and milestones.

As a project proceeds, the organizations involved will change. The plan should clarify the role/responsibility of the organization within each activity, in terms of:

- specifying requirements,
- completing the work,
- verifying the work meets the requirements.

The plan should only contain what is achievable within schedule and budget constraints. If it is necessary to omit previously identified activities, this should be with clear justification and understanding of the potential consequences (of carrying unmitigated risk).

5.4 Implementing the Plan

The process of implementing the activities at each project stage will involve breaking down the plan into a series of tasks or actions.

These actions need to be tracked and closed out to ensure completion.

As activities are completed, they should be checked against the previously stated goals and requirements to provide assurance that the identified technical risk has been addressed to a sufficient degree for the project stage.

In the early stages of a project, the activities may identify more new technical risks and associated actions which need to be addressed in the same way as the original risks.

Throughout the project, implementation activities provide assurance that:

- potential failure modes that could affect system performance have been analyzed and managed;
- all design decisions are consistent with the RM goals;
- the qualification of equipment has addressed the RM required by the project;
- all documented lessons learned from previous projects have been incorporated;
- the supply chain is fully integrated in to the reliability and technical risk management program;
- the achieved RM performance will allow production, financial and corporate performance goals and requirements to be met.

Implementation of the plan is supported, through the application of good management practices as described in 5.6.

5.5 Feedback

The feedback step provides the formal presentation of information to support decision making at the end of each project stage and also to assist other projects at earlier stages.

At the end of each stage, a documented record should exist of:

- activities completed,
- key findings,
- implemented measures.

This will provide assurance that the technical uncertainties have been addressed (or if not, why not).

A review of the work done is also completed to identify lessons learned such as:

- technical risks, failures or unwanted events which were not anticipated (but should have been);
- risks that were overestimated and why;
- successes that can be applied to other projects;
- suggested improvements, in the light of experience, in how to complete given activities (resource, schedule, etc.).

The feedback step establishes whether the project stage reliability goals and requirements have or have not been met and includes the success to which the required qualification activities have been implemented.

Feedback from operations to projects is also extremely important. Lessons learnt from operations regarding reliability performance of equipment should be included as an input to projects.

5.6 Supporting Reliability Key Processes (KPs)

These KPs provide a supporting environment for the reliability activities. When these are implemented across an organization the reliability and technical risk management effort for each project is reduced (good practice which had to be specified now happens automatically). Elements of each of the KPs are captured within the specific reliability activities described in Section 6 and Annex A. The theory and implementation of each of the 12 reliability KPs are detailed in Annex B.

The supporting reliability KPs are as follows.

KP 1—Definition of Availability Goals and Requirements ensures that the project goals are fully aligned with overall business performance objectives and provides the focus for design and manufacture for availability and reliability assurance. The trade-off between the purchase cost and the operational expenditure needs to be understood when considering the need for reliability (or maintainability) improvement. This should then be considered when setting goals and requirements (see B.1 for more details).

KP 2—Organizing and Planning for Availability allocates leadership and resources to the required reliability activities such that they add value to the project overall and do not adversely impact on the project schedule. The reliability activities identified should be considered an integral part of the engineering process and integrated with conventional engineering tasks in the project management system (see B.2 for more details).

KP 3—Design and Manufacture for Availability should be considered an extension of good engineering practice but requires increased focus on understanding how and why failures occur in operation. Information gathered during reliability analysis activities should be considered during the design process to drive the design's ability to achieve and deliver the specified availability requirements (see B.3 for more details).

KP 4—Reliability Assurance is the essential element of managing technical risk as it is the process of identifying, assessing, justifying and, most importantly, communicating the information pertaining to risks to the technical effectiveness of the system.

The key output from the reliability assurance process is the RAD. The purpose of the RAD is to provide the customer with evidence of progressive achievement of the reliability goals and requirements during the project (see B.4 for more details).

KP 5—Risk and Availability Analysis provides reliability management support by identifying failure modes/logic, consequences and the frequency of occurrence. Analysis and models usually focus on function, hardware or process. The specific type of assessment will depend on the amount of information available (i.e. the project stage), the subject of the analysis and the source of technical uncertainty. The output from the analyses enables clear prioritization of required activities and actions to minimize risk and optimize reliability/availability (see B.5 for more details).

KP 6—Verification and Validation confirms that any given activity is the correct one and that it has been carried out correctly (see B.6 for more details).

KP 7—Project Risk Management addresses non-technical risks throughout the project life cycle to enable all risks to be identified, quantified, managed and preferably eliminated (see B.7 for more details).

KP 8—Reliability Qualification and Testing is the process by which systems are examined and evidence is provided to demonstrate that the technology employed meets the specified requirements for the intended use. The qualification process in some projects may start as early as the feasibility stage if it is known that a specific piece of unqualified hardware will be required to exploit a field (see B.8 for more details).

KP 9—Performance Tracking and Data Management collects and organizes reliability performance data from all projects at all project stages to support the assessment of reliability, availability and production efficiency. Historical reliability and availability data can be used to determine the availability goals and requirements for projects with field

proven equipment, and also understand any failures that have been experienced to provide inputs to reliability analysis and improved design (see B.9 for more details).

KP 10—Supply Chain Management ensures that reliability and technical risk management goals, requirements, achievement and lessons learned are communicated between all organizations involved in the project (see B.10 for more details).

KP 11—Management of Change ensures that any changes (to scope, design, plan, etc.) are consistent with the project reliability and technical risk management goals and their impacts are fully assessed and managed (see B.11 for more details).

KP 12—Organizational Learning provides a common framework to capture an organization's learning on one project and communicate them back into the organization to be adopted by later projects. The lessons learned usually cover the whole life of the project from strategic thinking and decision making, through project execution and the delivery of benefits and should include both good and bad practice (see B.12 for more details).

The majority of organizations in the subsea industry practice many of these KPs in various forms; however, this RP provides information on key features of each process which promote good reliability and risk management practice.

5.7 Summary

The *Define, Plan, Implement and Feedback* loop is repeated for each stage of the project (see Figure 2) and within any given activity that has been identified as a necessary scope of work at each project stage.

All activities will generally fall within one or more of the KPs defined above. When the appropriate process is identified, further information and guidance is available within Annex B on each KP. The relationship between the *Define, Plan, Implement and Feedback* loop and the 12 KPs is shown in Figure 3.

The level of effort and number of KPs employed should be consistent with the level of risk identified for the given project. Figure 4 provides a representative example to the level of effort, but each project should develop their own plan to suit the application.

NOTE The project risk categories used in Figure 4 refer to the categories adopted in ISO 20815, an alternative method of risk categorization using "technical risk categorization" is presented in Annex A.

6 Recommended Practice for Each Project Stage

6.1 General

This section provides a general approach to achieve a desired reliability performance within projects.

6.2 Technical Risk and Reliability Effort

The first activity in every project stage should be an assessment of technical risk and uncertainty.

This should be a formal process to ensure consistency across different projects.

The process should:

- consider all sources of technical uncertainty that could impact the ability to achieve required performance;
- be carried out by experienced engineers who understand the project engineering scope at each project stage;

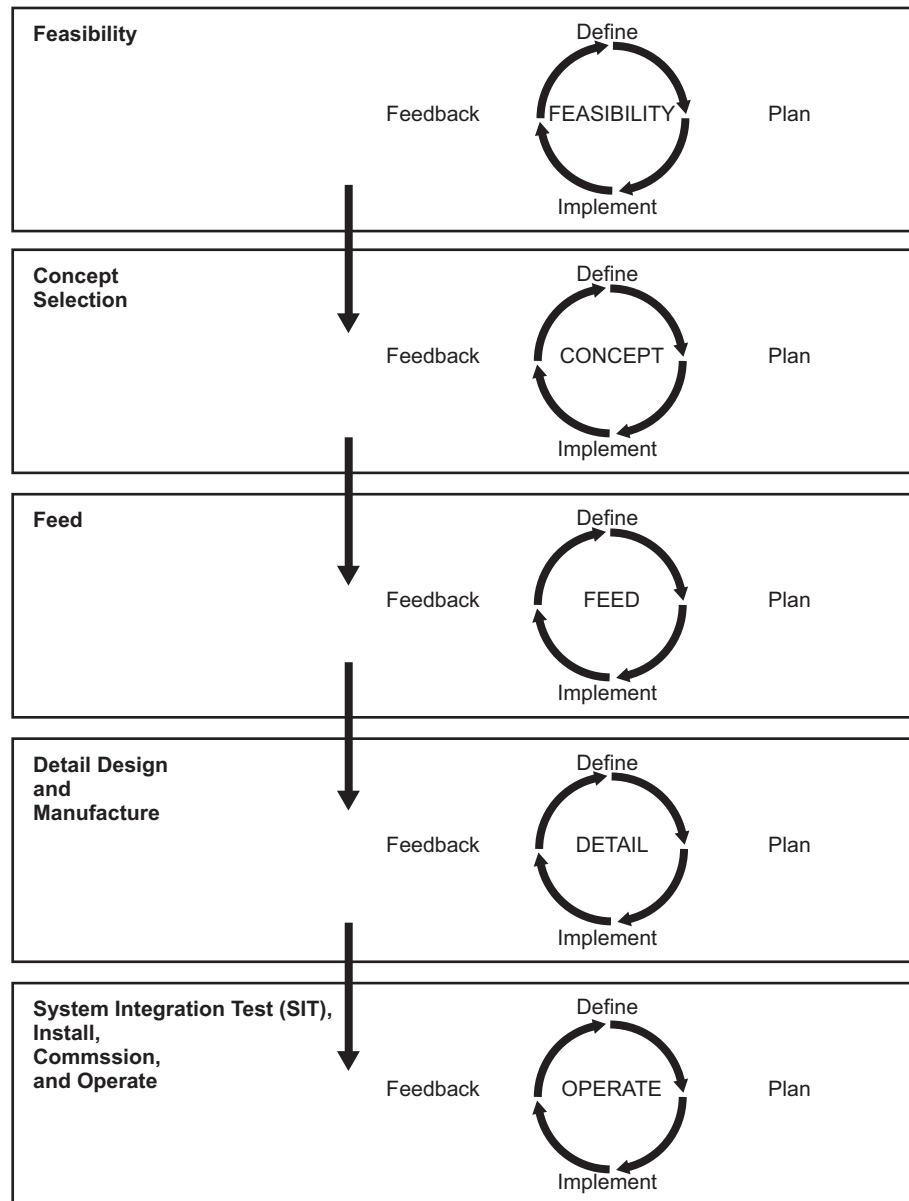


Figure 2—Project Life Cycle

- provide a qualitative “score” of risk to facilitate prioritization of mitigation effort (e.g. the method in Annex A uses categories A, B, C, D);
- adjust the level of focus from an overall project assessment to a detailed component assessment as the project develops from feasibility to design and manufacture.

More detailed reliability effort is recommended for projects/equipment involving high technical uncertainty. Whereas for projects/equipment involving low technical uncertainty (e.g. using field proven hardware), little reliability effort is expected beyond good engineering and management practices.

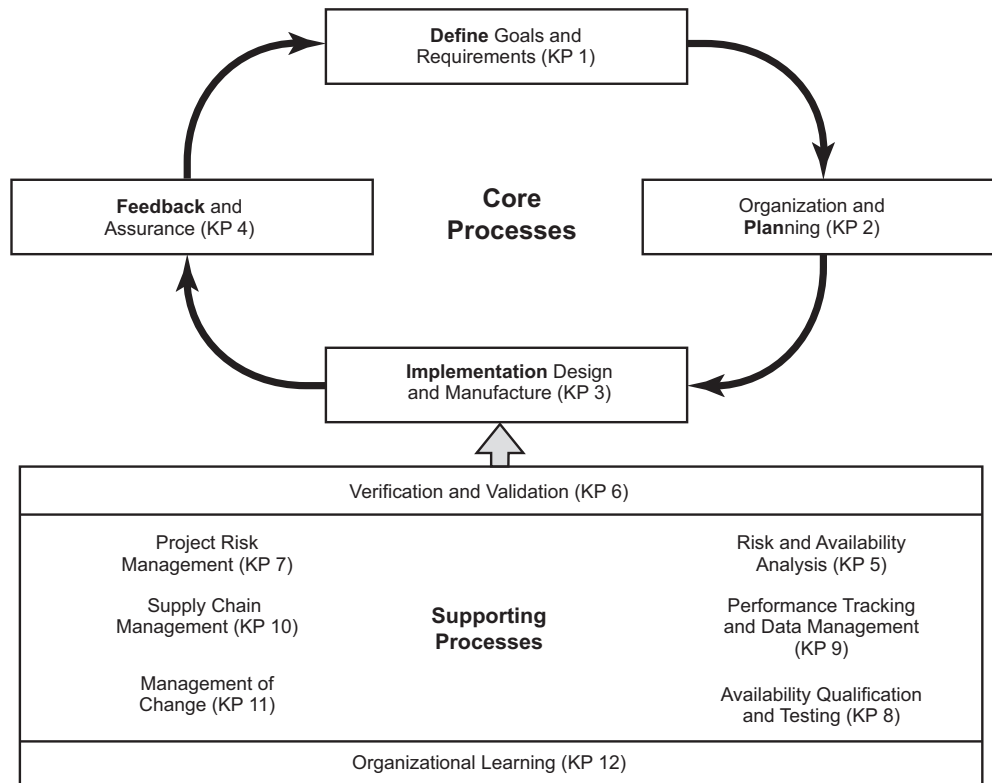


Figure 3—Key Process (KP) Interaction with Define, Plan, Implement, and Feedback Loop

6.3 Feasibility Stage

Reliability and technical risk management should contribute to the assessment of project feasibility relative to overall business strategy.

6.3.1 Define Goals, Strategy, and Requirements

The goal is project specific and should be determined by the project team and recorded. It should be a simple statement of what the project has to achieve in terms of technical (reliability) performance.

The goal should be translated into clear requirements to be met before the project can proceed to the concept selection stage.

The strategy is to assess the project technical risk and develop an appropriate scope of work to confirm that the project is feasible and commercially viable.

6.3.2 Define (Identify) Technical Risk

Undertake an assessment of technical risk at an overall project level. The technical risks to project feasibility will arise where key parameters are different in some way from previous experience. The parameters considered as potential sources of uncertainty should include:

- physical environment (in terms of pressures, temperatures, water depths and seabed conditions, etc.);

Assurance Processes for Asset Development				Life Cycle Phase						
Project Risk Categories			Main Processes	Pre-contract Award		Post-contract Award				
Low Risk Projects	Medium Risk Projects	High Risk Projects		Feasibility	Concept Selection	Front End Engineering Design (FEED)	Detailed Design and Manufacture	System Integration Test (SIT)	Install and Commission	Operate
	X	X	Definition of Availability Goals and Requirements	X	X	X	X			
X	X	X	Organizing and Planning for Availability	X	X	X	X	X	X	X
X	X	X	Design and Manufacture for Availability		X	X	X	X		
X	X	X	Reliability Assurance	X	X	X	X	X	X	X
	X	X	Risk and Reliability Analysis	X	X	X	X			
X	X	X	Verification and Validation	X	X	X	X	X	X	X
X	X	X	Project Risk Management	X	X	X	X	X	X	X
		X	Qualification and Testing		X	X	X	X		
X	X	X	Performance Data Tracking and Analysis					X	X	X
	X	X	Supply Chain Management			X	X	X	X	
X	X	X	Management of Change		X	X	X	X	X	X
X	X	X	Organizational Learning	X	X	X	X	X	X	X

Figure 4—Guide to Process Effort by Project Phase and Risk

- company experience, industry experience of similar developments;
- novelty of technology that may be needed;
- reliability expectations to meet financial goals.

Low risk projects are well understood with known and acceptable reliability based on the historical performance of similar projects.

Higher risk projects contain significant technical uncertainty in terms of how the project goals will be achieved.

6.3.3 Define Scope of Work

A scope of work that can be accomplished within the feasibility stage should be predefined for each risk level for all projects (to achieve consistent outcomes).

The scope of work should establish that the project is technically and commercially feasible and should consider the following:

- qualification status across all potential suppliers for the project environments;
- potential qualification effort and related schedule impact, if any;

- system availability expectations; whether they are consistent with the project financial goals and achievable with available technology.

The scope of work should be reviewed and adjusted as necessary for relevance to the specific project under consideration to ensure:

- the requirements for feasibility (define goals, strategy and requirements) will be met;
- that all risks identified have an associated scope of work to address them;
- the level of effort is consistent with the perceived risk.

6.3.4 Plan

A simple table identifying activity, deliverables, resources, due dates and means of verification should be sufficient at this stage. It is important that activities are planned so that they can directly influence feasibility decisions.

6.3.5 Implement

When feasibility engineering is nearly complete, the technical risk level should be revisited to identify if the original assessment has been altered by any new information. If the project risk has changed, then the new risks should be addressed and appropriate actions implemented.

6.3.6 Feedback

All information generated from the feasibility scope of work should be collated into a RAD.

The information presented within the RADs should provide a critical review of project technical feasibility (within commercial and schedule constraints). This shall confirm that:

- the scope of work identified has been completed,
- the technical risks identified can be managed within the project schedule and budget,
- the technical strategy for the project satisfies the project's financial objectives.

Feedback step should also report any lessons learned that could be of benefit to future projects including lessons learnt from previous operations.

6.4 Concept Selection

Reliability and technical risk management during concept selection is at the overall subsea **system level** and contributes to the selection of the system design.

At this point, a number of potential concepts have been identified and concept selection engineering is undertaken to identify the **best value** concept for the project.

6.4.1 Define Goals, Strategy and Requirements

The project reliability goal should be reviewed by the project team to confirm continued relevance. Any change should be recorded.

The goal should be translated into clear (reliability) requirements to be met by the selected concept (before proceeding to FEED). This may be in the form of a percent availability or similar.

The strategy is to undertake a technical risk assessment for all potential system concepts and then undertake the work scope to evaluate each concept option in terms of benefits and risks to determine the best value option.

6.4.2 Define (Identify) Technical Risk

Undertake an assessment of technical uncertainty of each system concept. Technical risks to potential system concepts will arise where key parameters are different in some way from previous experience. The parameters considered as potential sources of uncertainty should include:

- required operating environment (in terms of pressures, temperatures, water depths and seabed conditions, etc.) relative to previous experience;
- the relative novelty of technology in each concept;
- how system configuration deviates from previous practice;
- company experience, industry experience of using similar systems in similar applications;
- current expected system reliability compared with project reliability requirements.

Low risk concepts are well understood with known and acceptable reliability based on the historical performance of similar systems in similar applications.

Higher risk concepts contain significant technical uncertainty in terms of how the project goals will be achieved using that concept.

Activities defined in the scope of work should be performed to the level necessary to enable decisions on concept selection to be made.

6.4.3 Define Scope of Work

The scope of work that should be applied to each system concept should be predefined for each risk level for all projects (to achieve consistent outcomes).

The scope of work should establish technical and commercial value for each concept to the project and should consider the following:

- a system level functional FMECA to predict reliability performance of new (high risk) technology/systems or to provide relative comparison between competing systems;
- ability of the system concepts to meet the reliability and technical requirements (e.g. by simple RAM analysis);
- reliability requirements for the constituent subsystems derived from the overall concept requirements (e.g. derived from the simple RAM analysis);
- qualification status of each subsystem;
- relative qualification effort in terms of cost and schedule between concepts;
- potential cost/benefit (or value) of developing improved reliability performance;
- preliminary project execution plans to address differences in execution risk;
- thru-life cost/benefit comparison of options.

The scope of work should be reviewed and adjusted as necessary for relevance to the specific project under consideration to ensure:

- the requirements for concept selection (define goals, strategy, and requirements) will be met;
- that all risks identified have an associated scope of work to address them;
- the level of effort is consistent with the perceived risk.

6.4.4 Plan

A simple table identifying activity, deliverables, resources, due dates and means of verification should also be sufficient at this stage. The plan should be split by system concept with high risk concepts given more effort than low risk ones. The plan should ensure that activities are scheduled so they can directly influence concept selection decisions.

6.4.5 Implement

Activities defined in the scope of work should be performed according to the plan.

When concept engineering is nearing completion, the technical risk category of each concept should be reviewed to confirm the original assessment has not been altered by new information. If the concept risk has changed, then new risks should be addressed in the same manner.

NOTE Concepts may be dropped before the completion of their plan if new information reveals that the concept is no longer technically or commercially viable.

6.4.6 Feedback

All information generated during concept selection should be recorded and collated into a RAD.

The information presented within the RAD should provide a critical review of the risks and rewards for each option and how the risks can be managed (within commercial and schedule constraints). This review shall identify the option that best satisfies the concept selection criteria by demonstrating that:

- the scope of work identified has been completed,
- the recommended option provides the greatest opportunity to meet the project's financial objectives,
- the technical risks identified for the recommended option can be managed within the project schedule and budget.

Feedback step should also report any lessons learned that could be of benefit to future projects including lessons learnt from previous operations.

6.5 Front End Engineering Design (FEED)

Reliability and technical risk management during front end engineering is at the subsea **package (or subsystem) level** (e.g. tree system, control system, etc.).

NOTE Packages should ideally be identified so that each will eventually be supplied by a single supplier (i.e. no inter-company interfaces within any packages).

At this point, a concept has been selected and preliminary engineering is undertaken to confirm functionality and performance can be delivered at the expected cost. A key deliverable is usually package specifications for tendering to suppliers.

6.5.1 Define Goals, Strategy, and Requirements

The project reliability goal should be reviewed by the project team to confirm continued relevance. Any change should be recorded.

The strategy is to undertake a categorization for each package and then undertake the work scope to develop the functional and reliability requirements (specifications) for suppliers. For higher risk packages, these requirements may be a performance requirement (e.g. percent availability), or it may be a scope of reliability analysis (e.g. FMECA) to demonstrate all potential failure modes have been addressed. These specifications may include instructions to carry out the work scope described in 6.5.3.

Reliability requirements for the project subsystems have been determined at the concept selection stage; these should be further developed during FEED to establish the requirements on the constituent delivery packages.

6.5.2 Define (Identify) Technical Risk

Technical risk of all packages should be assessed at the start of FEED relative to previous project experience with similar systems.

The assessment should compare known project parameters against predetermined change risk factors as for the earlier stages.

As a result of this process, it should be clear that the reliability requirements on each package is within known supplier capability with known and acceptable reliability (low risk) or contains significant technical uncertainty in terms of capability or performance (high risk) for the application.

6.5.3 Define Scope of Work

The scope of work for each package should be predefined for each risk level for all projects (to achieve consistent outcomes). The deliverable for each package scope of work should be a document which details the package requirements in terms of:

- functional requirements for equipment,
- reliability requirements for the package,
- scope of reliability analysis to be carried out in detailed engineering, if appropriate.

NOTE Where packages represent low risk, reliability requirements may be assured by specification of field proven equipment.

The scope of work required to develop this requirements document should consider:

- the qualification status of the package,
- package availability goals to meet required system availability,
- relevant lessons learned from previous projects and operations,
- RAM data on package equipment,

- the capability of potential contractors and suppliers to effectively assess and deliver against the reliability requirements,
- use of a system level functional FMECA to predict reliability performance where new technology/systems means there is no useful performance data,
- a project execution plan and schedule to address organizational risk.

NOTE The above scope of work is generic and is guidance only; project teams shall ensure that all potential risk in each package is addressed.

6.5.4 Plan

A brief project document identifying activity, deliverables, resources, due dates and means of verification is recommended at this stage.

The plan should be split by package and subsystem with high risk items given more effort than low risk ones. The plan may be a compilation of individual package plans developed by each package engineer; if so the complete plan should be reviewed and agreed by all parties prior to execution. The plan(s) should ensure that activities are scheduled to directly influence the final system design and requirements for suppliers.

Some level of independent verification (the means by which it will be confirmed that each activity has been completed correctly, e.g. third party review or organized peer review) is appropriate at this stage.

6.5.5 Implement

Activities defined in the scope of work should be performed according to the plan.

When FEED is nearing completion, the technical risk category of each package should be reviewed to confirm the original assessment has not been altered by new information. New risks should be addressed in the same manner as original ones.

6.5.6 Feedback

All information generated during FEED should be collated into a RAD.

The information presented within the reliability assurance document should provide a critical review of the risks and benefits for the proposed system and how these risks will be managed (within commercial and schedule constraints). This review shall demonstrate that:

- the scope of work identified has been completed,
- all requirements on suppliers of equipment have been identified and are consistent with overall system design reliability requirements and the project's overall financial objectives,
- the technical risks identified for each package can be managed within the project schedule and budget.

Feedback step should also report any lessons learned that could be of benefit to future projects including lessons learnt from previous operations.

6.6 Detail Design and Manufacture

Reliability and technical risk management during detailed design and manufacture is at the subsea **component (or subassembly) level** (e.g. valve, connector, control pod, etc.).

At this point, suppliers have been selected for each package and responsibility for meeting reliability requirements transfers to them as they undertake detailed engineering and manufacture.

6.6.1 Define Goals, Strategy and Requirements

The overall project goal remains unchanged at this stage. In addition to meeting purchaser's goals, suppliers may have their own goals for the project execution. These should be determined by the supplier project team and recorded.

The strategy is to undertake a technical risk assessment which considers each component/subassembly and then undertake the necessary work scope to demonstrate the functional and reliability requirements are met.

Reliability requirements for each package have been determined at the FEED stage; the supplier is now responsible for demonstrating that they have been met through the design and verification of the equipment delivered.

6.6.2 Define (Identify) Technical Risk

It is assumed that prior to this stage the equipment list for each package has been identified. The technical risk of all subassemblies or components should be assessed at the start of detailed engineering relative to previous project experience with similar systems, subsystems and subassemblies.

The assessment should compare known project parameters against predetermined change risk factors as for the earlier stages.

As a result of this process, it should be clear that the reliability requirements on each item is within its capability (low risk) or contains significant technical uncertainty in terms of capability or performance (high risk to reliability) for the application.

The end user (operator) of each subassembly/component should agree these assessments.

6.6.3 Define Scope of Work

The scope of work for any given component should be predefined for each risk level for all projects (to achieve consistent outcomes).

A specific scope of work should be developed for each component from the generic activities defined for each risk level and should consider as a minimum:

- use of detailed component FMECA to understand potential failure modes and drive design reliability improvement of high risk components,
- assessment of each component's qualification status against project functional and reliability requirements and completion of any outstanding qualification activities (see B.8, Process 8—Reliability Qualification and Testing and API 17Q or DNV RP A203),
- formal incorporation of lessons learned from previous projects,
- final system level RAM analysis to confirm overall availability performance will meet expectations with the actual components selected,
- use of independent expert reviews of the design,
- use of peer reviews/lessons learned reviews including those from relevant operations to add experienced input to the design.

The scope of work should be split by package and subsystem and the level of effort should be consistent with the perceived risk.

NOTE 1 Design teams shall ensure that all activities address the source of risk in each component (and are agreed between supplier and end user).

NOTE 2 Operators may also specify a scope of work to be carried out by suppliers during detailed design if appropriate.

6.6.4 Plan

Plan should identify how the full scope of work will be managed including specific resource to verify reliability work is completed at the right time and all lessons learned and actions identified have been incorporated into manufacturing instructions and closed out before delivery.

A detailed project document identifying activity, deliverables, resources, due dates and means of verification should be developed for each package by the supplier in response to the reliability requirements specification and agreed by the end user (operator) prior to execution. Suppliers should consider incorporating the reliability plan into the project execution plan, to ensure that reliability activities link to and influence other project activities.

The plan should specify how each activity will be validated and verified (the means by which it will be confirmed that the correct activity has been selected to match the risk and that it has been completed correctly).

Independent validation and verification e.g. third party review or organized peer review, is recommended for high risk items.

6.6.5 Implement

Activities defined in the scope of work should be performed according to the plan with regular monitoring of progress and compliance (by supplier and end user).

The technical risk category of each component should be reviewed at agreed intervals to confirm the original assessment has not been altered by new information (e.g. changes in design, materials or coatings). New risks should be addressed in the same manner as original ones.

Prior to delivery of equipment, the plan should be used as a punch list to confirm all planned activities have been completed to the satisfaction of both parties.

6.6.6 Feedback

All information generated during detailed design and manufacture should be collated into a RAD for each delivered package.

The information presented within the RAD should demonstrate that:

- the scope of work identified has been completed,
- the proposed system design will meet the client's reliability requirements (and hence their financial objectives),
- the technical risks identified for each package have been managed by supplier to the end user's satisfaction (the assurance document should be a deliverable from supplier to end user).

Feedback step should also report any lessons learned that could be of benefit to future projects including lessons learnt from previous operations.

6.7 System Integration Test (SIT), Install, Commission and Operate

Reliability and technical risk management during SIT, installation, commissioning and operations is at the **procedural level** (e.g. SIT procedure, installation procedures, etc.).

This phase of effort should be initiated when supplier is well underway with detailed design, but in advance of the SIT, etc. being carried out. Detailed procedures will need to be written to ensure that all equipment is operated correctly and within its acceptable limits.

Where appropriate, procedures should specify key performance data to be collected and fed back into future reliability assessments. This is particularly (but not exclusively) relevant to integrity management procedures.

6.7.1 Define Goals, Strategy and Requirements

The overall project goal probably remains unchanged at this stage.

However, specific SIT, installation, commissioning and operations goals should be developed to ensure the installation or operation of the equipment will not compromise reliability (by avoiding/controlling any actions which could cause immediate or later failure). In addition to meeting purchaser's goals, suppliers and installers may have their own goals for the project execution. These should be determined by the individual teams and recorded.

The strategy is to undertake a technical risk assessment of each procedure and then undertake the necessary work scope to demonstrate all requirements for reliability have been included.

Reliability requirements for each component have been determined during detailed design; the installer is now responsible for demonstrating that all procedural requirements for the installation and operation have been captured (some of which may be output from the design reliability analyses).

6.7.2 Define (Identify) Technical Risk

It is assumed that prior to this stage the procedure list (and scope of equipment covered within each procedure) for each package has been identified. The technical risk associated with each installation or operating procedure should be assessed.

The assessment should compare known project parameters against predetermined change risk factors as for the earlier stages (different operations from previous experience).

As a result of this process, it should be clear whether the planned procedure is conventional and understood (low risk) or contains significant operational uncertainty (high risk to reliability) for the application.

The end user (operator) of each component should agree these assessments.

6.7.3 Define Scope of Work

A specific scope of work should be developed for each procedure to ensure creation of the (or review of the existing) procedure receives inputs and reviews appropriate to the level of risk. This should consider:

- use of a process FMECA to identify potential failures that could occur during each step of the procedure with a view to finding better (risk reducing) ways of completing the task (high risk operations only),
- confirm that all procedure-related actions from any detailed design FMECA and peer reviews are incorporated,
- use of final multi-discipline review by an independent entity (to the project and the supplier) with direct installation experience of similar systems (high risk operations only),
- use installation procedures during SIT to identify problems and improvements,

- confirm all outstanding qualification tests have been completed and incorporate any implications for installation and operation,
- use previous stage FMECA and RAM analysis to ensure integrity management procedures take account of reliability critical equipment and highest probability failure modes,
- a mechanism to record problems and improvements in the field (particularly but not exclusively) on first use and update procedures accordingly,
- installation team experience and training (e.g. consider involvement in SIT).

The level of effort should be consistent with the perceived risk.

NOTE 1 The project installation team shall ensure that all activities address the source of risk in the procedure (and are agreed between supplier and end user).

NOTE 2 Any issues identified in any of the procedure reviews should be considered in the context of the other procedures, to ensure that changes identified in one area are consistently addressed in all other related areas.

6.7.4 Plan

A brief project document identifying activity, deliverables, resources, due dates and means of verification should be sufficient.

It is possible that examination of procedure may reveal design improvement, it is, therefore, recommended to write and review procedures before manufacture is too far advanced.

6.7.5 Implement

Activities defined in the scope of work should be performed according to the plan with regular monitoring of progress and compliance (by supplier and end user).

6.7.6 Feedback

All information generated during SIT, installation, and commissioning and operations should be collated into the RAD for each delivered package.

The information presented within the RAD should demonstrate that:

- the scope of work identified has been completed,
- the proposed installation and operational instructions will not compromise the design reliability of the equipment,
- the potential procedural failures identified for each procedure have been managed by supplier to the end user's satisfaction (feedback report should be a deliverable from supplier to end user),
- integrity management philosophy and practice is tuned to the reliability requirements and the results of reliability analysis in terms of component criticality and potential failures.

Feedback step should also report any lessons learned that could be of benefit to future projects (e.g. better ways of doing things that were only apparent after operations have commenced).

Annex A **(informative)**

Technical Risk Categorization Approach to Reliability and Technical Risk Management

A.1 General

This annex provides an example of one method to systematically organize the key practice described in Section 6 using a technical risk categorization technique to define appropriate level of activity for each project stage.

NOTE The generation of goals and creation of implementation plans for each stage is not repeated (see Section 6 for these details).

A.2 Technical Risk Categorization

Technical risk categorization is common to all design stages of a project (from project categorization in feasibility through to component categorization in detailed design). It occurs towards the beginning of every project stage and is a qualitative assessment of a number of “change risk” factors that can influence the likelihood of failure.

Five change risk factors have been defined (reliability, technology, architecture, environment and organization) that are assessed against four different levels of risk based on the perceived deviation from previous experience. The levels of risk for each change risk factor are defined in Table A.1.

It is essential that categorization be carried out by experienced engineers who understand the project engineering scope at each project stage.

Ground Rules

Categorization should not be an onerous activity. The following ground rules are used to facilitate the process.

- If there is any doubt as to which technical risk category applies, select the higher risk category (and investigate the uncertainty).
- The selected level of risk for each change factor should be accompanied with brief explanation/justification of the risk category to aid future understanding.
- The overall category for the project/package/equipment is the highest of the categories for the individual risk change factors.
- The definitions in Table A.1 are general and are intended to be applied at project, package, and component level. Some interpretation for each project stage and project scope may be necessary.
- The definitions in Table A.1 are guidance; detailed project knowledge may supersede this with recorded justification.

This categorization activity does not consider criticality. The scope of work for each category may, therefore, be revised if it does not add value, e.g. a novel sensor may result in a Category A (high technical risk), but its failure may have little effect on overall system operability. The reliability effort (for a Category A component) may, therefore, be adjusted to reflect this situation (with written justification).

Table A.1—Technical Risk Categorization

	Technical System Scale and Complexity			Operating Envelope	Organizational Scale/Complexity
	Reliability	Technology	Architecture/ Configuration	Environment	Organization
Key Words	- Reliability requirements - Maintainability - Availability - Failure modes - Risk - Uncertainty	- Materials - Dimensions - Design life - Design concept - Stress limits - Temperature limits - Corrosion - Duty cycle	- Equipment - Layout - Interfaces - Complexity - Diver/ROV - Deployment/ intervention - Tooling	- Field location - Water depth - Seabed conditions - Reservoir conditions - Environmental loadings - Test location - Storage	- Location - Company - Contractor - Supply chain - Design - Manufacture - Install - Operate - Maintain
A (Very high)	Reliability improvements (technology change): A significant reliability improvement requiring change to the technology involved.	Novel technology or new design concepts: Novel design or technology to be qualified during project.	Novel application: Architecture/ configuration has not been previously applied by supplier.	New environment: Project is pushing environmental boundaries such as pressure, temperature, new part of world, severe meteorological conditions or hostile on land test location.	Whole new team: New project team, working with new suppliers in a new location.
B (High)	Reliability improvements (design change): Significant reliability improvement requiring change to the design but no change to the technology.	Major modifications: Known technology with major modifications such as material changes, conceptual modifications, manufacturing changes, or upgrades. Sufficient time remains for qualification. Non mature for extended operating environments.	Orientation and capacity changes: Significant architectural/ configuration modifications such as size, orientation and layout; changes fully reviewed and tested where viable. Large scale, high complexity.	Significant environmental changes: Many changes noted; extended and/or aggressive operating environment; risk requires additional review.	Significant team changes: Project team working with new supplier or contractor within supply chain; key technical personnel changes from previous project.
C (Medium)	Minor reliability improvements: Reliability Improvements requiring tighter control over quality during manufacture assembly and fabrication.	Minor modifications: Same supplier providing a copy of previous equipment with minor modifications such as dimensions or design life; modifications have been fully reviewed and qualification can be completed.	Interface changes: Interface changes, either with different equipment or control system changes; where appropriate, configuration has been tested and verified.	Similar environmental conditions: Same as a previous project or no major environmental risks have been identified.	Minor team changes: Small or medium organization; moderate complexity; minor changes in contractor/supplier and project team.
D (Low)	Unchanged reliability: No reliability improvements required, existing quality assurance (QA) and control is acceptable.	Field proven technology: Same supplier providing equipment of identical specification, manufactured at same location; provide assurance no changes have occurred through the supply chain.	Unchanged: Architecture/ configuration is identical to previous specifications; interfaces remain unchanged, with no orientation or layout modification.	Same environmental conditions: Same as recent project.	Same team as previous: Same project team, contractors, suppliers, and supplier's supply chain; applies throughout project life cycle.

A.3 Feasibility Stage

Reliability and technical risk management during feasibility is at the **project** level and supports the assessment of project feasibility relative to overall business strategy.

A.3.1 Define (Identify) Technical Risk

Experienced engineers should review Table A.1 and consider where the potential project lies in terms of reliability, technology, system architecture, environment and planned project organization.

The output from their review is a project category (A through D) which best represents the technical risk as understood at the start of feasibility engineering work.

Category A projects will be characterized by a high level of **uncertainty**, for example, in terms of:

- pressures and temperatures of produced fluids are beyond previous experience for the development (suggesting a high level of new design and qualification will be required);
- the technology and environment may be relatively standard, but the project team is inexperienced and is located remote from the primary technical resource of the company.

Category D projects will be characterized by a high level of **certainty** in terms of environments very similar to existing projects, high likelihood of being able to use standard field proven equipment and an experienced project team with a good understanding of technical requirements and how to achieve them.

A.3.2 Define Scope of Work

The scope of work has been defined for each project category as follows.

Feasibility—Scope of Work
Category A and B Projects — For each area of technical uncertainty the qualification status shall be determined across all potential suppliers (at this stage, this should be at the system level, but may focus on key equipment that is the source of the uncertainty). — Suppliers of equipment should be contacted to establish the effort in terms of cost and schedule to develop a qualified system. This shall then be built into the preliminary project schedule with enough float to account for the accuracy of the information. — Establish a system availability goal that is consistent with the project financial goals and achievable with the technology. This may require consultation and iteration with several groups e.g. project finance, technical experts. A review of previous extended technology projects may also give an indication of what reliability can realistically be achieved. — Where uncertainty exists over the project organization a preliminary project execution plan shall be prepared to address the potential risk. This may involve changing project team location to be able to better access a company knowledge base, or involve relocating key experience to the remote project location.
Category C and D Projects — Establish a system availability goal that is consistent with the project financial goals and achievable with the technology. This should be a straightforward task of ensuring previous performance will meet financial expectations.

NOTE The above scope of work is generic for the project category and is for guidance only; project teams shall ensure that all risks identified have an associated scope of work to address them.

A.3.3 Feedback

Feasibility—Reliability Assurance Document (RAD)

All information generated from the feasibility scope of work should be collated into a RAD, which should contain statements on:

- goals, requirements and strategy;
- project technical risk category;
- description of work carried out and findings;
- claims relating to project feasibility and expected reliability performance including expected qualification effort, system availability requirements and technical justification on how it will be achieved;
- recommendations for the project;
- the capture of lessons learned for future stages and other projects.

A.4 Concept Selection

Reliability and technical risk management during concept selection is at the overall subsea **system level** and contributes to the selection of the system design.

A.4.1 Define (Identify) Technical Risk

It is assumed that prior to this stage all potential system concepts have been identified.

The responsible engineering team should review Table A.1 and consider where each system concept lies in terms of reliability, technology, system architecture, environment and planned project organization.

The output from their review is a project category (A through D) for each system concept which best represents the technical risk as understood at the start of conceptual design work.

Different concepts may have different technical risk categories reflecting the differing levels of technical uncertainty for each concept and hence the different scope of reliability effort that will be required.

A.4.2 Define Scope of Work

Concept Selection—Scope of Work
Category A and B Concepts
— For each system concept the qualification status should be estimated. The effort in terms of cost and schedule to develop a qualified system for each system concept should be established. — Review the system concepts against the system availability goal and assess their ability to deliver this (or better) performance (e.g. by simple RAM analysis). A system level functional FMECA to identify major technical risks can be used to predict reliability performance of new technology/systems or to provide relative comparison between competing systems. — For any concepts where expected reliability does not meet commercial goals, consider if improvements in reliability are possible. This may require consultation with technical experts and potential equipment suppliers. The cost and benefit of any improvements should be included in the overall commercial comparison of options. NOTE Improved designs may also need to be qualified (see first item). — For any concepts where uncertainty exists over the project organization and its supply chain, develop a concept specific project execution plan to address the risk. Any financial impact should be included in the overall commercial comparison of options. — For each system concept, a preliminary project schedule and value analysis should be completed to compare thru-life cost reflecting the reliability and qualification status of the concept and the benefits and costs of developing it for the project. This should ensure that the option selected is of optimum value to the owner.
Category C and D Concepts
— Confirm the system concepts can achieve the project availability goal with reference to previous similar systems. Actual relevant performance data are preferred to generic historical data. — For each system concept, a preliminary project schedule and thru-life cost/value should be completed (to provide like for like comparison against A and B concepts). Actual costs are preferred to previous estimates.

NOTE The above scope of work is generic for the concept stage and is for guidance only; project teams shall ensure that all activities address the source of risk in each concept.

A.4.3 Feedback

Concept Selection—Reliability Assurance Document (RAD)

All information generated during concept selection should be collated into a RAD, which should include:

- goals, requirements and strategy;
- technical risk category for each concept;
- description of work carried out for each concept and findings;
- claims relating expected reliability performance of each concept and confidence with which performance can be achieved. (including any future actions on which performance depends e.g. qualification testing);
- value/thru-life cost benefit analysis and assumptions behind the analysis;
- concept selection recommendations for the project.

A.5 Front End Engineering Design (FEED)

Reliability and technical risk management during front end engineering is at the subsea **package (or subsystem) level** (e.g. tree system, control system, etc.).

NOTE Packages should ideally be identified so that each will eventually be supplied by a single supplier (i.e. no inter-company interfaces within any packages).

A.5.1 Define (Identify) Technical Risk

Prior to this stage assumptions would have been made about the basic layout of the subsea system and its constituent packages e.g. cluster or template layout, types of equipment to be used, key features required, etc.

The project engineering team should review Table A.1 and consider where each package lies in terms of reliability, technology, system architecture, and environment and planned project organization.

The output from their review is a project category (A through D) for each package which best represents the technical risk as understood at the start of FEED.

A.5.2 Define Scope of Work

A specific scope of work should be developed for each package from the generic activities defined for each technical risk category as outlined below.

FEED—Scope of Work
Category A and B Packages
— Confirm the qualification status of the package and develop a first draft of the test program to be carried out by suppliers of that package. By this means, the effort in terms of cost and schedule to develop a qualified system for each system concept should be further clarified. — Carry out a system level RAM analysis to confirm that overall performance will meet expectations. NOTE The RAM model needs to be defined by package level, so results can be interpreted by package. — Consider the need for availability improvements by investigating the through field life cost/benefits of different configuration options, any relevant project lessons learned, including those from relevant operations, should be considered. Assess the benefit of a reliability based maintenance strategy. — After any improvements are incorporated, use the RAM analysis to identify availability expectations on each package (rationalized by historical data) and include in package functional specification to be sent to suppliers. NOTE The requirement in the specification should be for this availability to be demonstrated by the supplier. Suppliers which do not have RAM analysis capability should be asked to provide the necessary data (see B.9) so others can undertake analysis (may be part of a later detailed system RAM analysis). — The reliability capability of potential contractors and suppliers to effectively assess and deliver against the reliability requirements should be considered as part of the supplier selection process along with the standard selection criteria (see B.10.2). — Where new technology/systems means there is no useful performance data a system level functional FMECA should be used to predict reliability performance. This is also useful in developing a qualification test program which matches tests with potential failure modes (to confirm they have been designed out) (see B.8).

- For any package where uncertainty exists over the project organization and its supply chain, develop a package specific the project execution plan to address this risk. Any financial/schedule impact should be included in the overall commercial assessment and requirements for equipment suppliers should be added to project execution requirements specification for tendering (e.g. percent local supply, skills requirements for local supplier, etc.).
- For each package, a subassembly level project schedule and thru-life cost comparison should be completed which reflects the reliability and qualification effort identified through the work above (and may account for different supplier's equipment). The project execution plan or similar should also identify how the full scope of work will be managed.

Category C and D Packages

- Review the packages against the reference systems they are based on to confirm that performance data from the reference system is still relevant. Any relevant lessons learned, including those from relevant operations, should also be considered. If additional changes are required, the bullets above apply. Actual relevant performance data is preferred to generic historical data.
- For each package, a subassembly level project schedule and thru-life cost comparison should be completed which reflects the reliability and qualification effort identified through the work above. The project execution plan or similar should also identify how the full scope of work will be managed.

NOTE The above scope of work is generic and is guidance only; project teams shall ensure that all activities address the source of risk in package.

A.5.3 Feedback

FEED—Reliability Assurance Document (RAD)

All information generated during FEED should be collated into a RAD, which should include:

- goals, requirements and strategy;
- technical risk category for each package;
- description of the work carried out for each package and findings;
- claims relating expected reliability performance of each package and confidence with which performance can be achieved (including any future actions on which performance depends e.g. qualification testing, reliability analysis);
- reliability requirements for suppliers (performance targets for equipment and scope of work during design and manufacturing) including equipment selection recommendations/requirements;
- thru-life cost benefit analysis and assumptions behind the analysis;
- report of any lessons learned that could be of benefit to future projects.

A.6 Detail Design and Manufacture

Reliability and technical risk management during detailed design and manufacture is at the subsea **component (or subassembly) level** (e.g. valve, connector, control pod, etc.).

At this point, suppliers have been selected for each package and they undertake detailed engineering to enable manufacture. The detailed design is required to meet client reliability and functional requirements.

A.6.1 Define (Identify) Technical Risk

It is assumed that prior to this stage the equipment list for each package has been identified.

The package design team (supplier or subcontractor) should review Table A.1 and consider where each component lies in terms of reliability, technology, system architecture, environment and planned project organization.

The output from their review is a project category (A through D) for each package which best represents the technical risk as understood at the start of detailed design and manufacture.

The end user (operator) of each component should agree these assessments.

A.6.2 Define Scope of Work

A specific scope of work should be developed for each component from the generic activities defined for each technical risk category as outlined below.

Detailed Design and Manufacture—Scope of Work
Category A Components
— Undertake a detailed component FMECA to identify potential failure modes and define clear actions/mitigations to improve design reliability (see B.5, Table B.8). Lessons learned from previous projects, including those from relevant operations, should be incorporated in this analysis. Additional mitigations/monitoring/control to be adopted in Integrity Management in operations should also be considered (i.e. expand the FMECA results to develop a reliability based maintenance strategy where inspection and monitoring frequency is based on a risk of failure assessment). — Undertake a detailed assessment of each component's qualification status to confirm that all unqualified equipment has a defined test program which meets all project functional and reliability requirements within the project delivery schedule (see API 17Q). Implement the qualification program as appropriate to enable the required qualification status to be achieved at the right time in the project. — Carry out a final system level RAM analysis to confirm overall performance will meet expectations. NOTE RAM model needs to reflect actual components to be used in its build, so results can be interpreted by component (and weak links identified). — In addition to any project design reviews, invite external experts (to the project and the supplier) to review and challenge the design and its assumptions at 80 % complete. — For any component where uncertainty exists over design team experience consider altering team or increasing peer reviews/lessons learned reviews, including relevant operational experience, to add experienced input to the design. — The project execution plan or similar should also identify how the full scope of work will be managed including specific resource to verify reliability work is completed at right time and all actions identified have been closed out before delivery.

Category B Components

- Undertake a detailed assessment of each component's qualification status which confirms that all (unqualified) modifications to equipment have a defined test program which meets all project functional and reliability requirements within the project delivery schedule (see API 17Q). Start to implement the qualification program as appropriate to enable the required qualification status to be achieved at the right time in the project.
- Carry out a final system level RAM analysis to confirm overall performance will meet expectations.

NOTE RAM model needs to reflect actual components to be used in its build, so results can be interpreted by component (and weak links identified). RAM model may also be used to inform sparing, intervention and maintenance strategies.

- Modify the detailed parent component FMECA to take account of the major modifications made and identify all new potential failure modes to improve design reliability (see B.5, Table B.8).

NOTE Modifications may introduce new failure modes in unchanged parts of a design if they are subject to different loads, environment, etc. as a result. If an existing FMECA is not available then this should be created.

- The FMECA should also be reviewed to identify any additional mitigations/monitoring/control to be adopted in Integrity Management in operations.
- In addition to any project design reviews, invite external (to the project) experts, including relevant operational expertise, to review and challenge the component design and its assumptions at 80 % complete.
- For any component where uncertainty exists over design team experience consider altering team or increasing peer reviews to add experienced input to the design.
- The project execution plan or similar should also identify how the full scope of work will be managed including specific resource to verify reliability work is completed at right time and all actions identified have been closed out before delivery.

Category C Components

- Undertake a detailed assessment of each component's qualification status which confirms that all notionally qualified equipment is backed up by the test record which shows that the test is to the same standard as the project requires and the tested components are the same unit as proposed for the project.
- Review the packages against the reference systems they are based on to confirm that performance data from the reference system is still relevant. If not, the bullets above apply. Actual relevant performance data is preferred to RAM analysis predictions.
- Verify that the detailed parent component FMECA is still applicable for the new component with minor changes. If an existing version is not available, the project should consider the value of creating one for this project.
- In addition to any project design reviews, invite external (to the project) experts, including relevant operational expertise, to review the overall system design at 80 % complete.

Category D Components

- When all detail design is at approximately 80 %, verify that all components are exactly as used previously (if not, the categorization should be raised and the activities above become relevant).

NOTE The above scope of work is generic and is guidance only; design teams shall ensure that all activities address the source of risk in each component (and are agreed between supplier and end user).

A.6.3 Feedback

Detailed Design and Manufacture—Reliability Assurance Document (RAD)

All information generated during detailed design and manufacture should be collated into a RAD for each delivered package, which should include:

- package reliability requirements;
- technical risk category for each component in the package;
- resultant reliability scope of work carried out by the supplier;
- description of the work carried out for each component (A, B and C only) and findings;
- claims relating expected reliability and qualification performance of each package and confidence with which performance can be achieved;
- summary reports of any reliability analysis (e.g. FMECA or external peer review) including list of actions identified;
- positive confirmation that actions were addressed and closed out;
- report of any lessons learned that could be of benefit to future projects.

A.7 System Integration Test (SIT), Install, Commission and Operate

Reliability and technical risk management during SIT, installation, commissioning and operations is at the **procedural level** (e.g. SIT procedure, installation procedures, etc.).

The reliability activities relating to SIT, installation, commissioning and operations start before the end of detailed design. At this point, suppliers have been selected for each package and detailed design is well underway. Detailed procedures are being written to ensure that all equipment is operated correctly and within its acceptable limits. The activity also affects eventual field reliability and, therefore, must be addressed.

A.7.1 Define (Identify) Technical Risk

It is assumed that prior to this stage the procedure list (and scope of equipment covered within each procedure) for each package has been identified.

The package design team (supplier or subcontractor) should review Table A.1 in the context of the relevant procedures, and consider where each procedure scope lies in terms of reliability, technology, system architecture, environment and planned (installation and operation) organization.

The output from their review is a project category (A through D) for each procedure which best represents the technical uncertainty/complexity of each procedure (risk) as understood at the start of procedure creation.

The end user (operator) of each component should agree these assessments.

A.7.2 Define Scope of Work

A specific scope of work should be developed for each procedure from the generic activities defined for each technical risk category as outlined below.

SIT, Install, Commission and Operate—Scope of Work	
Category A and B Procedures	
—	The reliability capability of potential installation contractors to effectively assess and deliver against the reliability requirements should be considered as part of the contractor selection process along with more the more standard selection criteria (see B.10.2).
—	Undertake a process FMECA to identify potential failures that could occur during each step of the procedure and alter procedure to remove each failure possibility (see B.5). Whenever possible, each procedure step should include a positive record that action was carried out correctly; for critical operations this may include additional witness.
—	Confirm that all procedural related actions from the previous stage FMECA, peer reviews and qualification requirements are incorporated (part of previous stage actions close out) into the relevant procedures.
—	The final procedure should be reviewed by external experts (to the project and the supplier) with direct installation experience of similar systems.
—	Installation procedures should be used as much as possible during SIT to identify problems and improvements.

- Review assumptions and output from previous stage FMECA and RAM analysis to ensure that all decisions concerning integrity management (or maintenance strategy) are appropriate and acceptable to the achievement of reliability.
- A mechanism should be set up to record problems and improvements in the field (particularly but not exclusively) on first use and procedures updated accordingly (a wash-up meeting after first installation is a common method to achieve this).
- For any procedure, where uncertainty exists over installation/operations team experience consider altering team or providing additional training (e.g. involvement in SIT).

Category C and D Procedures

- The final procedure should be reviewed by the personnel with direct installation experience of the previous similar (parent) systems.
- Installation procedures should be used as much as possible during SIT to identify problems and improvements.
- Review assumptions and output from previous stage FMECA and RAM analysis to ensure that all decisions concerning integrity management are appropriate and acceptable to the achievement of reliability.
- A mechanism should be set up to record problems and improvements in the field (particularly but not exclusively) on first use and procedures updated accordingly (a wash-up meeting after first installation is a common method to achieve this).

NOTE The above scope of work is generic and is guidance only; design teams shall ensure that all activities address the source of risk in the procedure (and are agreed between supplier and end user).

A.7.3 Feedback

SIT, Installation, Commissioning and Operations—Reliability Assurance Document (RAD)

All information generated during SIT, installation, commissioning and operations should be collated into a RAD for each delivered package, which should include:

- list of procedures and scope of equipment addressed by each,
- technical risk category for each procedure written,
- resultant procedure improvement scope of work carried out by the supplier,
- summary of improvements identified and incorporated (process FMECA summary),
- positive confirmation that actions (including actions from design reliability analysis and qualification requirements) were addressed and closed out (final procedure),
- report of any lessons learned that could be of benefit to future projects (e.g. better ways of doing things that were only apparent after operations commenced).

Annex B (informative)

Detailed Reliability Process and Activity Description

This annex provides specific guidance on how to perform the tasks identified in Annex A, in terms of the 12 KPs (with reference to existing standards where relevant). The annex also describes the supporting management activities/processes recommended to support reliability implementation.

B.1 Process 1—Definition of Availability Goals and Requirements

B.1.1 Description

The definition of availability goals and requirements ensures that the project is congruent with overall business performance and provides the objectives for design and manufacture for availability and reliability assurance.

The definition of availability goals and requirements will generally follow the assessment of technical uncertainty. It is recommended that the following two aspects are addressed:

- defining hardware availability goals and requirements,
- defining requirements on management activities to achieve availability.

Value (cost benefit) analysis should be incorporated and integrated in the definition of availability goals and requirements, to ensure the trade-off between the purchase cost and the operational expenditure of an item is understood when considering the need for reliability (or maintainability) improvement. This should then be considered when setting goals and requirements.

B.1.1.1 Hardware Availability Goals and Requirements

Availability goals and requirements initiate the reliability plan and ensure that the project is congruent with key business performance metrics (e.g. financial, environmental, health and safety). These requirements may also direct the project strategy towards reliability or maintainability.

- **Goals and requirements:** It is important for the project team to distinguish between a goal, which it should aim to achieve, and a requirement, which shall be met as a condition of contract.
- **Quantitative (numerical) hardware availability goals and requirements:** These will usually be specified as Availability goals rather than as contractual requirements. As a general rule, high level Availability goals and requirements should align with the operators business objectives. For some projects there may be a minimum Availability requirement specified as a production availability or production efficiency value. This will normally require a higher availability for the subsea system to achieve the overall field requirement. These high level availability goals and requirements are allocated to packages as the project progresses such that each package should have an Availability goal or requirement specified. In many cases the specified availability goal will be a failure rate based on the historical failure rate, with no specific requirement for improvement. In addition to failure rate data, all packages and components will have functional and performance requirements which should also be related to the availability goals and requirements.

An example of a performance requirement for a subsea seal might take the form: subsea seal should withstand a pressure of 5000 bar. An associated reliability requirement for this example might be: subsea seal should withstand a pressure of 5000 bar with a probability of intervention for replacement in the first 2 years of less than 2 %. This is essentially an MFOP example.

- **Qualitative (non-numerical) hardware availability goals and requirements:** Qualitative goals and requirements may focus on engineering actions or provide a qualitative goal for numerical analysis. For example, the following qualitative availability goals and requirements may be imposed on an engineering contractor or supplier:
 - supplier is required to take appropriate actions to reduce the risk of failure from specified failure modes,
 - contractor is required to maximize system availability,
 - contractor is required to design hardware with low reliability to be retrievable,
 - supplier is required to implement manufacturing and assembly improvements to improve reliability.

For lower technical risk projects, the availability goals and requirements will usually refer to historical performance or supplier specifications, provided that these meet business objectives.

For higher technical risk projects, availability goals and requirements may require the reliability performance of some packages to be stretched e.g. to meet an overall availability goal or requirement. In other cases, suitable historical data may not be available and reliability may need to be estimated in other ways, e.g. using predictive models or by reliability testing.

Qualitative availability goals and requirements focus engineering activity to operational parameters such as failure definition, workaround philosophies and strategies. They may also focus design parameters such as fault tolerance and redundancy.

B.1.1.2 Management Activity Requirements to Achieve Availability

Goals and requirements on management activities to achieve availability address the management processes and practices that deliver product reliability. The Reliability Tasks are fundamental to the implementation of a reliability strategy. Operators, their contractors and suppliers are expected to have competent personnel for performing these reliability tasks.

- **Qualitative (non numerical) goals and requirements on management activities to achieve availability:** These will represent the majority of goals on management activities and may include, for example, where an operator may wish to impose a goal or a requirement for a contractor or a supplier to apply specific reliability techniques on certain equipment, such as: RAM analysis, FMECA, RBD, FTA, ETA, etc.
- **Quantitative (numerical) goals and requirements on management activities to achieve availability:** For some high risk projects the supplier or contractor capability may require quantification. For example, an operator may require the contractors and suppliers to achieve an acceptable reliability capability level (e.g. Level 4) within the project. The capability maturity of the contractor should be assessed using an agreed reliability capability maturity model.

B.1.2 Reliability Value Analysis

Reliability value (cost benefit) analysis is performed as part of the goals and requirement setting process. The purpose of the analysis is to assess the value of investing in the availability of particular packages in a system. This requires an assessment to be made of the CAPEX, OPEX and income arising from production and its dependence on reliability, maintainability and intervention logistics.

The reliability of hardware packages has significant impact on operational expenditure. Package reliability improvement may decrease OPEX, decrease deferred production losses and hence increase field value. Set aside from this there may be increased CAPEX associated with realizing reliability improvements. For example, additional costs may be incurred in performing analyses, tests and making product improvements.

Reliability value analysis can be undertaken either qualitatively (by expert judgment) or quantitatively (by implementing life cycle costing methods) and provides a means for cost benefit assessment for reliability centered decision making in design and manufacture.

Quantitative reliability value analysis provides a means of assessing the system architecture, over the project life cycle, in terms of the financial risks attributed to either complete or partial failure of the functional requirements. The economic risk associated with the technology is determined by combining conventional discounted cash flow analysis with a system reliability assessment. In order to generate the annual expenditure a model is required to track failure events and assign failure cost data.

There are many uncertainties associated with the economic performance of an oil field development. As such, reliability value analysis should be subject to validated simplification assumptions. Consequently, reliability value analysis should not be considered as a method of full economic appraisal and should only be used as a method of comparative analysis.

B.1.3 Outline Procedure for Defining Availability Goals and Requirements in Projects

This section recommends a procedure for defining the availability goals and requirements for hardware suppliers and design contractors to meet in detail design and manufacture.

B.1.3.1 Principles

- **Align availability goals and requirements to business objectives:** Availability goals and requirements provide the fundamental objectives of technical risk management in field development projects. It is important that the high level performance measures and availability goals and requirements are realistically aligned with over-arching business objectives.
- **Value added goals and requirements:** Availability goals and requirements should be specified to enable project value to be enhanced. It is important to understand the relation between investment in reliability and the overall benefits this brings to the project.
- **Understanding numerical availability goals and requirements:** Numerical reliability and availability performance should be specified as a goal rather than as a requirement and used to support decision making to optimize project performance.
- **Using models and expert judgment to support decision making:** The use of valid reliability/availability models and data can assess the reliability impact of design change and the scope for value improvement. Expert judgment may form an important input to these assessments, especially if historical data is inadequate.
- **Defining availability requirements for supplier specification:** When the system design is shown to meet the overall availability goal, the model input data become, in effect, the availability goals for the items comprising the model. RAM models should be defined at a level to generate the required output data. For example, the RBD for the RAM model should be broken down only as far as items at the package level if the operator is looking to specify availability requirements to a package supplier. The package supplier, however, will need to use package availability models with data inputs at a components level. The supplier will be required to provide evidence of reliability achievement to the operator reliability goal. This may require further modeling with validated data. Where package components are bought in, the model data will in turn become the goal for the components. These goals may, where appropriate, be imposed on second or third tier suppliers.

B.1.3.2 Recommended Procedure

The definition of availability goals and requirements for submittal in a customer specification can be defined through an optimization process as outlined in Figure B.1. This process observes a double feedback/optimization loop where technically feasible design and strategy solutions are first assessed against high level availability criteria and secondly against a functional/financial value criteria.

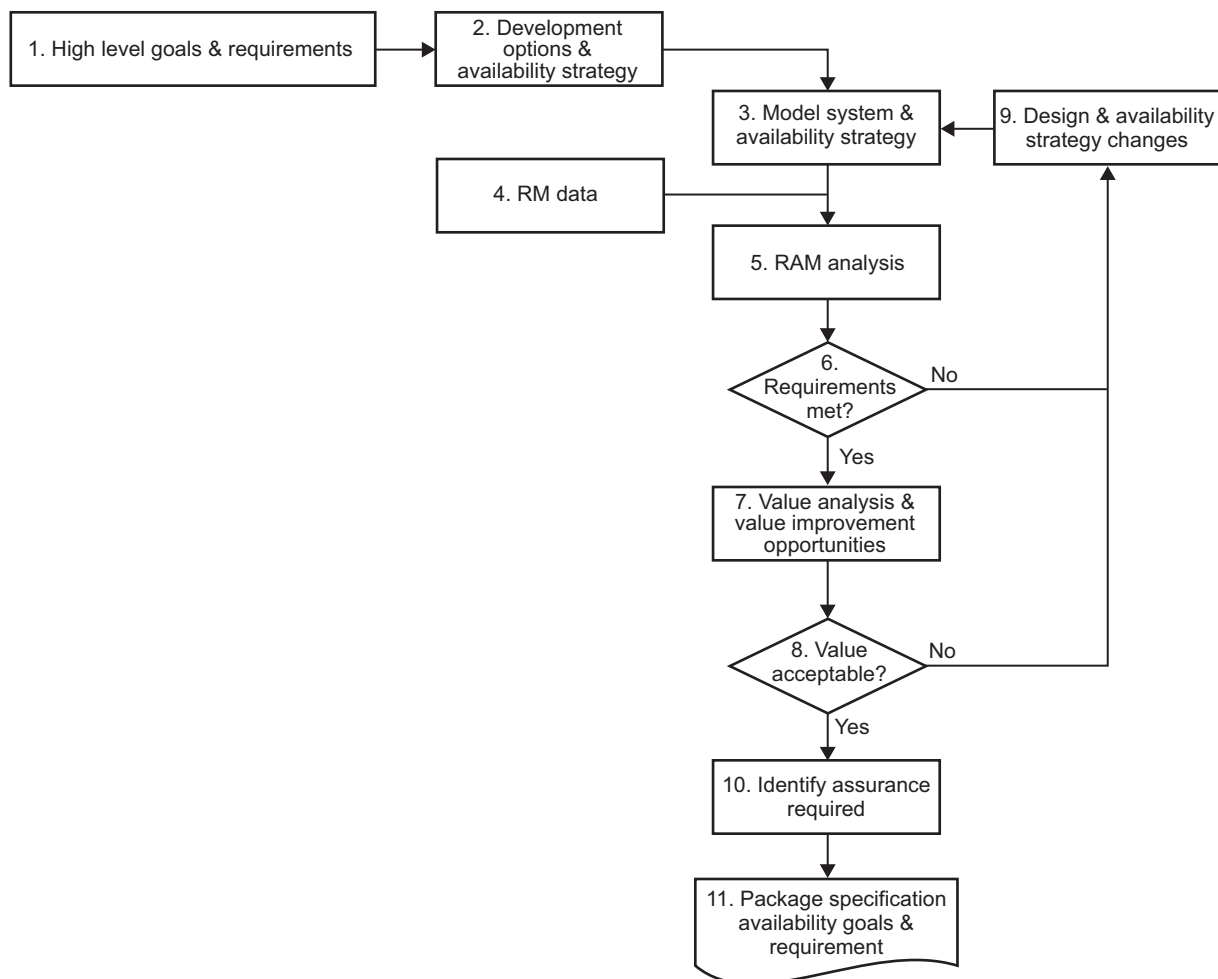


Figure B.1—Procedure for Defining Availability Goals and Requirements

- **High level goals and requirements:** Define the availability performance and acceptance criteria that satisfy the business objectives. Example metrics are given in Table B.1. The influence between the surface and subsea systems should be considered to ensure the business objective is achieved. This provides the minimum availability requirement for the subsea system in order to deliver the business objective. Availability goals may be specified that are greater than the minimum Availability requirement.

Table B.1—Availability Performance Metrics Example

Metric	Description
Availability	Directly related to the system's ability to generate revenue. When addressing 'availability' it is vital to define which availability the measure is referring. System availability may not return the same value as production availability.
Maintainability	Metric aimed at reducing the time to return a failed system back to the production state.
MFOP	Metric used to specify the period during which no system failures occur requiring maintenance (usually during the early life period), with an associated acceptable probability.
Reliability	Metric aimed at increasing the time that a system is in the production state.

- **Development options and availability strategy:** Identify feasible options for the field development and define the focus of the availability strategy (reliability versus maintainability) capable of delivering the high level goals and requirements.
 - A maintainability strategy should consider low reliability items, spare part inventories and the ease of keeping or restoring the system to an operational state.
 - A reliability strategy may be required when the cost of failure is unacceptable. A reliability strategy should consider the introduction of redundancy, additional qualification effort or greater quality control in manufacture.
- **Model system and availability strategy:** Create a model which represents the system reliability logic and the Availability strategy. Reference should be made to KP 5 (Risk and Availability Analysis) to identify a suitable technique for logically representing the system and Availability strategy. Typically modeling will be in the form of a RBD. Many commercial RAM analysis tools include RBD capability. The model should be sufficiently detailed to reflect the maintenance and intervention policies. Careful consideration should be given to the assumptions built into the model. The detail and scope of the modeling effort depends on the project stage.
 - During concept selection there should be a system model for each development option (and availability strategy where appropriate).
 - The selected concept should be further detailed in FEED. This may be achieved by nesting more detailed reliability models within the concept selection model or by updating the input data (see below).
- **RM data:** Input valid historical data where practicable. Generic data may be available through databases such as OREDA or PARLOC. More specific data may be implemented either from the operator's databases or supplier specifications. Where specific data are not available, analyses may be required to estimate this. Input data should adequately reflect any uncertainty in the data. When populating the model with RM data, consideration should be given to relevant maintenance times and logistic delays (e.g. global vessel availability and mobilization times). The detail of the RM data should increase depending on the project stage.
 - During concept selection, RM data are likely to be more generic with broader acceptable uncertainty.
 - During FEED, RM data should be more specific focusing on the availability performance of specific items rather than larger systems or subsystems. This data may be obtained directly from potential suppliers.
 - During detailed design, the RM data should be updated to reflect the supplier's design specification.
- **RAM analysis:** Once a model (e.g. RBD) of the system has been created and populated with appropriate RM data, RAM analysis can be performed. For oil and gas production systems, production availability models which include a model of the field production profile are recommended as this is the best method of connecting the production performance with the availability performance of the installed equipment.
 - Large complex systems often require tools utilizing Monte Carlo simulation (MCS) methods. MCS also facilitates the evaluation of parameter uncertainty on defined performance measures. The analysis should identify those items to which the system performance is most sensitive.
- **Evaluate the system against availability goals and requirements:** Compare the output from the RAM analyses with Availability goals and requirements (acceptance criteria). If the design, strategy and item RM data satisfies the acceptance criteria, then the process should continue on to the next phase of the goal setting

procedure (value analysis) otherwise changes to the design or strategy may be required. The evaluation depends on the project stage.

- In concept selection, the evaluation against the acceptance criteria should be used to support the decision regarding which concept is to be detailed in FEED. The output from the analysis can be used to update the minimum requirements and support future evaluations.
- In FEED, the evaluation should be used to support the decision regarding the necessity of performance improvements (either through design changes or strategy modifications).

It is recommended that historically available reliability data such as that published in OREDA be used initially and that initially only system architecture is addressed. In other words, try initially to meet production availability goals using published reliability data (failure rates)

- **Value analysis and value improvement opportunities:** Investigate the impact of availability performance on project value. This requires the definition of a value metric (see Table B.2) and associate value goal. Assessing the project value requires an estimation of the associated costs (and revenue if required). As with RAM analysis, value analysis should identify those items which are most sensitive to value improvements.

Table B.2—Value Metrics Examples

Metric	Description
Financial Value	Financial metrics used in financial investment decision making. Examples include net present value (NPV), internal rate of return (IRR) or life cycle cost (LCC). Reference should be made to ISO 15663-2, which provides guidance on the financial evaluation techniques and decision making criteria.
Functional Value	Functional value is a measure of functional performance divided by the cost required to deliver performance. The decision making criteria for functional value is usually one of value maximization.

- **Evaluate project value:** As a method for comparing design options, a reliability based decision criteria may be formulated. Table B.2 provides guidance on the acceptance criteria for value options. Design and availability strategy options should be assessed against this criteria and a decision made regarding the acceptability of this value. The sensitivity of the system and system elements to the value metric should be assessed and reviewed to ascertain the scope for value improvements.
- **Design and availability strategy changes:** Many changes to a project's system architecture, its design or strategy are related to technical or flow assurance considerations rather than a direct function of reliability. All proposed changes should be validated by a technical expert and assessed by further RAM analysis (and value analysis where appropriate). This includes updating the system reliability model and the input data.
 - Modifying the system layout requires that the system logic for the RAM model be updated.
 - Strategies to reduce the maintenance time may require that the system logic be updated. Spare part inventories should be updated if the sparing policy is modified to reduce logistic delays.

If the system layout has been finalized but the predicted performance does not meet the acceptance criteria, then individual items may require reliability improvements (e.g. through the change of design or material of construction). While the RAM analysis may support the decision as to what the reliability improvement should be (by setting a reliability goal), it cannot support the engineering process of how to improve the reliability. This requires an expert judgment and detailed reliability analysis (physics of failure).

- **Identify assurance required:** Once the design and strategy have passed through the optimization process, the assurance requirements should be specified. The operator should specify the assurance required (depending on the technical risk) to support the contention that the requirements have been met and the extent to which the goals have been achieved.
- **Package specification and availability goals and requirements:** The package specification should be formalized to include the Availability goals and requirements as determined from the optimization process (i.e. the input data) and the specified assurance required by the Operator.

B.1.4 Defining Goals and Requirements in Detailed Design

Detailed design is a major transition from the operator to the supplier and may be the first direct involvement of the supplier in the field development process. It is essential for a smooth transition and successful design that clear, unambiguous and complete specifications are provided by the operator to the supplier. This is the major output from the RAM analyses performed during the FEED stage of the project and becomes an important availability specification input to the package supplier.

This specification should be reviewed and agreed between the operator and supplier. If changes to the specification are required (by either operator or supplier), then the new specification should be reviewed with direct regard to the effect of the changes on the overall system availability performance.

The goal and requirement setting process in detailed design is two-fold.

- **Allocating goals and requirements to specific items:** Translating the FEED specification into a detailed design specification requires the allocation of requirements to specific items. It is recommended that the package availability requirements imposed by the customer are allocated to subsystems and components using a similar approach to that outlined in Figure B.1 and described in B.1. There will be some differences in tools to be used. For example, if the supplier has been given a package availability as a specification to be met, a tool for modeling system availability will be more appropriate than a production availability tool. Likewise, if the availability goal is in the form of a reliability to be achieved then a system reliability tool, e.g. RBD, FTA or ETA may be used at a level for which historical and acceptable data is available (this should be agreed with the customer). If the system architecture delivers the required reliability then the RM input data become the component requirements. If the architecture cannot meet the availability specification then some component reliabilities will need to be stretched beyond that which is historically achieved. A description of a complete reliability allocation procedure is beyond the scope of this RP and it is recommended that reliability specialists be consulted to support the allocation process.
- **Defining manufacturing and assembly procedures:** Specify the availability requirements for hardware manufacture and assembly. These procedures should include the manufacture and assembly process requirements designed to ensure that the detailed design specification (above) is not compromised by defects and faults introduced during manufacture and assembly. These procedures, for example, may include a process FMECA, QA and control requirements in manufacture and may also include a variety of tests and actions to detect and eliminate faults. In some cases accelerated tests may be imposed. Each of these procedures should be reviewed, clarified and finalized (where necessary) prior to the initiation of the procedure in the relevant project stage.

B.1.5 Defining Goals and Requirements for Installation and Commissioning

Installation and commissioning failure modes and risks should be defined prior to installation and commissioning. The key goal is to implement these processes in such a way that the RM of hardware being installed and commissioned are not compromised. It is recommended that this is addressed through requirements to perform techniques which will reveal areas of installation risk such; technical risk categorization, operational risk assessment (which focuses task reliability) and FMECA for installation equipment where the installation has been categorized as A or B.

B.2 Process 2—Organizing and Planning for Availability

Implementation of KP 2—organizing and planning for availability, is extremely important through all project stages. It is recommended that this KP is always implemented regardless of the project risk category and is updated at the start of each project stage.

B.2.1 Description

The purpose of the organizing and planning process is to allocate leadership and resources to the required reliability activities such that they add value to the project overall and do not adversely impact on the project schedule.

The effort required is related to the level of technical risk and, therefore, it is the technical risk categorization that determines the scale of effort. The reliability activities identified should be considered an integral part of the engineering process and integrated with conventional engineering tasks in the project management system.

In planning for availability it is helpful to understand that the greatest value is achieved when:

- the reliability process is championed by, and has the full support of, senior management;
- project team is “incentivized” to achieve availability goals that deliver optimal value;
- availability strategy and availability goals and requirements are addressed early in the design process;
- sufficient resources (manpower, tools and time) are allocated to reliability activities;
- analysis is timely, quick, effective and most importantly informs decision making;
- design teams have good capability in “design for RM;”
- project plans and resources are flexible and enable reliability actions to be implemented and followed up.

B.2.1.1 Planning for Availability

A reliability plan is a definition of reliability activities and the resources required to deliver the availability goals and requirements. The plan is an important aspect of technical risk management; it should reflect the technical uncertainty inherent in the project and be updated as technical risks are better understood. Reliability planning starts at the feasibility stage of a project and is continuously updated through all project stages over the whole life cycle of the field development. Reliability plans should typically include the following information:

- the relevant technical risk categorization;
- availability goals and requirements;
- required activities (e.g. analyses, tests, design changes);
- resource and schedule demands;
- ownership (see below);
- references to internal/external standards and or practices.

The plan should support the construction of the reliability assurance documentation (see B.4) as it indicates how reliability value can be assessed, delivered and demonstrated. This process includes both planning the activities to deliver reliability value and allocation of tasks to task owners and participants.

The planning process has four primary drivers which influence the level of effort and the focus of the reliability activities; these are summarized in Table B.3 and should be considered during the planning process.

Table B.3—Primary Drivers and Influences for Planning for Availability

Driver	Influence
Business Objectives	Business objectives should reflect corporate strategy and as such influence project risk profiles and expectations on financial performance. Business objectives influence both the availability strategy and, more directly on the plan, the available resources for reliability activities.
Availability Strategy	The availability strategy directs the philosophy adopted to achieve the availability goals and requirements. The availability strategy may specify a low risk strategy benefiting from accumulated assurance for similar successful projects. Existence of accumulated assurance will reduce the analysis required and focus on maintaining the current levels of reliability and quality. A strategy of continuous reliability improvement would drive technical risk to a minimum of technical risk Category C which should in turn focus the effort on quality control and/or assurance. An operational strategy that focuses on maintainability implies that the assurance activity should likewise focus on maintainability issues such as ease of intervention, optimization of spares, availability of intervention vessels, etc.
Availability Goals and Requirements	Numerical availability goals provide a focal point for the reliability activities. The plan should reflect the nature of effort required in attempting to achieve the goals and allocate suitable resources. Availability requirements may explicitly quote activities to be included within the plan. The level of assurance required may also drive the respective effort (in terms of the amount of accumulated assurance).
Technical Risk Categorization	Technical risk categorization identifies areas within a project where changes from previously successful projects pose a risk to the achievement of availability goals and requirements. Technical risk categorization directs the effort to specific pieces of equipment and/or procedures of higher technical risk. The relative level of effort is also implied from the technical risk category (see A.2).

As inputs to the planning process, the availability strategy, goals and requirements and technical risk categorization should all be considered when allocating resources to reliability effort in field development projects. The technical risk categorization should be used to focus attention to equipment/procedures of high technical risk and direct the appropriate analysis techniques to the sources of technical risk (i.e. the change risk factors, see Table A.1). Guided by the technical risk categorization, the recommendations in the RM practice guide section and KP support provided in this annex, the plan should list all the activities considered necessary to deliver the availability goals and requirements and associated assurances.

It should be noted that throughout the field development project numerous options may be subject to the decision making process (e.g. in concept selection). In these cases it is important that an individual plan be allocated to each option so as to focus on the specific sources of uncertainty for that option. The construction of individual plans may themselves become a valuable input to decision making processes (e.g. in concept selection or when evaluating tender documents).

During allocation of reliability effort to specific reliability tasks, reference should be made to the importance of each task and the technical risk category. Adequate resources should be allocated to activities to ensure satisfactory completion. As the level of detail increases and the risk category increases so the planned effort for each task increases; this is observed both in terms of time to completion but also a shift towards increasingly more quantitative activities (see Table B.4).

Once the level of effort required and resources available for each task have been defined, the plan can be formulated with the aid of conventional project management tools and practices. BS 6079-1:2002 [4] provides an overview of project management techniques that can be adopted for the purposes of constructing the plan.

Table B.4—Guidance on the Level of Effort Required for Reliability Effort

Technical Risk Category	Nature of Assessment Work	Effort Expectation
A	quantitative	more
B	mostly quantitative/some qualitative	
C	some quantitative/mostly qualitative	
D	qualitative	less

For reliability planning the following guidelines are recommended.

- Operators should initiate reliability plans as early as possible in feasibility and concept selection stage. In later stages (e.g. after concept) plans should be adopted by contractors in consultation with the operator.
- Planning follows initial availability requirements definition.
- Plans should be updated during concept selection, FEED, detail design, manufacture and installation as the project progresses and details are defined.
- Reliability plans for a given stage may require actions to be initiated in an earlier stage and then updated during the active stage. For example, it is recommended that installation contractors are included in design reviews during FEED or detail design and installation plans and risk assessments are performed in advance of the installation stage e.g. during detail design or manufacture.
- Planning should anticipate that as the project evolves, unexpected failure modes and the need for further analysis may be required. Likewise, package risk categories may change as project progresses from concept selection to FEED and then to detail design. The plan should, therefore, be flexible, updatable and, where necessary, appropriate change actions enforced.
- The plan should:
 - identify how the availability is to be understood and demonstrated through the project life;
 - list all reliability activities that have been identified as necessary for the project, through all stages, with appropriate schedules, deliverables, milestones and resources allocated as appropriate;
 - anticipate that during each stage there may be some re-categorization of the project or package that may lead to new requirements/component and may create new reliability activity requirements;
 - reflect the technical risk associated with the project and that it is being properly implemented;
 - allocate sufficient resources to the initial categorization and reliability goal setting tasks;
 - be updated and issued periodically as new tasks (to be performed) or unnecessary tasks (to be deleted) are identified and defined in more detail.

- The document should include sections describing:
 - the reliability team and the roles and responsibility of the delivery manager and the discipline leaders;
 - the project/package/component categorizations at each stage of the project;
 - the availability requirements for the project, including both process and product requirements;
 - references to procedures or procedural requirements that should be followed in order to adhere to company requirements for:
 - reliability analysis,
 - project risk management,
 - management of change,
 - supply chain management,
 - lessons learned;
 - the reliability plan should include clear estimates of durations, costs and resources required to implement the necessary activities;
 - the reliability plans should be formally integrated with the design schedule.

B.2.1.1.1 Organizing for Availability

There are various approaches that may be adopted in organizing for availability. This will depend, amongst other things, on the size and scale of the project and the operator preferences. The following provides some guidance on the task of organizing for availability.

Three key questions arise when considering organizing for availability:

- Who is to be responsible for ensuring RM achievement?
- Who is to perform the analytical work?
- Who is responsible for coordinating RM activities?

As a general guidance, responsibility for ensuring reliability achievement should reside with the same senior managers responsible for ensuring the delivery of the subsea system to time and budget. Analytical tasks and coordination of reliability activities may be outsourced to reliability specialists if there are insufficient internal resources. However, it is crucially important that:

- reliability activities are fully integrated with engineering activities;
- analytical tasks inform design decision making;
- reliability decisions are followed up, acted on and closed out in a timely manner.

It is helpful to assign ownership to each of the reliability activities/tasks and to delegate responsibility for the implementation of the reliability activities. For a small project, a centralized approach may be acceptable. For a large project, with a large design team it will be necessary to assign specific areas of reliability responsibility and task

ownership at the various levels of technology indenture depending on the project stage. For example, the overall project manager may own the project reliability processes at feasibility and concept selection stage but once the project has progressed into FEED, package engineers can own the relevant reliability processes.

All of the upcoming reliability tasks should be resourced with the necessary and relevant expertise. For those reliability tasks that directly relate to or extend from existing engineering/business/organizational practices, the task should be resourced according to current organizational protocols with facilitation from a reliability specialist where necessary. For example, selecting a vendor would normally involve communication between operator and supplier; in order to account for reliability capability within the decision making process, support from a reliability specialist may be required. Where a task relates to a specific technology package, but not necessarily an existing engineering/business/organizational task, the package engineer should assume ownership with support from a reliability specialist where necessary. For example, if the technology risk categorization is for a new task; in this case, during FEED, the person(s) assigned ownership of the subsea control systems should undertake the risk categorization with support from a reliability specialist as necessary.

The following are examples of special reliability roles which operators, design contractors and suppliers may consider as part of their reliability organization. For some projects, the reliability specialists may have other important engineering roles in the project or may have a combined reliability role (more than one of these reliability roles).

- The reliability champion would ideally be a senior manager with authority and influence. His/her role would be primarily that of advocate and high level reliability problem solver. He/she would not necessarily be the person in control of the project.
- The reliability delivery manager would ideally be the subsea system delivery manager and be responsible for ensuring that adequate resources are available to meet reliability, cost and schedule requirements. However, he may delegate responsibility for meeting specific package reliability cost and schedule requirements to package leaders who would be responsible for managing the reliability activities in their area of responsibility but not necessarily perform them. For example, the lead pipeline engineer should own all of the processes associated with the availability of the pipeline, but would not necessarily be responsible for performing all specified reliability activities. Availability modeling of the pipeline, for example, might be contracted out or requested from the supplier.
- A specialist reliability engineer may often be required to support projects. The specialist should have specialist knowledge of tools and analytical techniques, combining good statistical and mathematical skills with knowledge of engineering hardware and failure mechanisms. The specialist's role is one of owning the tools and data and facilitating availability analyses (e.g. FMECA) and modeling (systems reliability models).
- Reliability assurance manager may be appointed to take responsibility for collation and integration of all relevant project availability outputs and its compilation into the RADs. This may be performed by internal project staff or may be outsourced to specialist reliability consultants.
- Availability verification and validation authority—This may involve internal staff or may involve independent external consultants.

B.3 Process 3—Design and Manufacture for Availability

B.3.1 Description

Delivery of a reliable subsea system requires attention to the KP 3—design and manufacture for availability, throughout concept selection, FEED, detailed design, manufacture and assembly. It should be considered an extension of good engineering practice but requires increased focus on understanding how and why failures occur in operation.

Given the information gathered during technical risk categorization, reliability value analysis, reliability analysis and modeling, risk based decisions should be made regarding the design and its ability to achieve and deliver the specified availability requirements. During the definition of availability requirements, it is usually necessary to determine whether the design focus is to be primarily reliability or maintainability or some combination in order to help prioritize design decisions.

B.3.1.1 Design for Availability

A relatively small proportion of products which fail in service are considered to be caused by errors in design. Nevertheless, it is very important for designers and original equipment manufacturers to provide sufficient resources in the design process to ensure that all failure modes have been identified and appropriate actions have been taken to reduce the probability of failure.

Design failures are invariably triggered by human error which may be in the form of mistakes or slips and lapses in the design process. In some cases mistakes are triggered by lack of knowledge of the underlying failure mechanism and in others it is caused by lack of knowledge of the application environment. A reliability focused design attempts to reduce the probability that a system will fail during the operational time in the specified operating conditions by paying particular attention to understanding failure modes and mechanisms and creating a design which is not susceptible to the failure mechanism, which is insensitive to design variation (e.g. in the environment, or dimensions) or which will tolerate faults or damage.

Different design actions may be taken at different stages in the design process. For example, during feasibility and concept selection, the focus will be on the overall system architecture with little consideration for the inherent reliability of specific packages and components. During FEED, designers attention will focus on system reliability and the identification of system failure modes and cut sets. At this stage, consideration should be given to redundancy and system common cause failures. In detail design, manufacturers and suppliers will drill down to component level failure modes. At this stage, more information should be available to identify common cause failure mechanisms and component failure mechanisms.

Examples of design for reliability considerations include:

- eliminating known failure modes,
- improvement of interface reliability,
- introduction of redundancy,
- reducing the probability of failure mode occurrence,
- removal of all common cause failures or reducing their probability of occurrence,
- simplification of the system and parts count reduction.

At component level design for reliability should address materials selection, stress, surface finish and environment issues. Typical considerations include:

- mechanical load and stress reduction (e.g. removal of stress raisers);

- dimensional tolerance stack up during assembly;
- increase mechanical strength (e.g. by selection of stronger materials or increased dimensions);
- fatigue resistance (e.g. material specification, surface finish);
- corrosion and stress corrosion cracking resistance (e.g. by selection of corrosion resistant materials);
- thermal stress and thermal fatigue.

Reliability analysis will provide useful support to engineering decisions. For example, systems reliability and value analysis can be used to help decide on the approach to reliability improvement, e.g. whether to adopt a redundancy strategy or whether it is better to select a more reliable supplier of a component.

For failures at component level, physics of failure and stress-strength interference models may be employed to support design improvement decisions. These tools are often more appropriate to support product development and qualification testing.

A maintainability focused design will attempt to improve the ease with which the system can be retained in, or restored to, a production state. Examples of design for maintainability considerations include:

- enable system inspection and condition monitoring,
- 'hot' intervention,
- improve interface accessibility,
- introduce modular design,
- introduce redundancy,
- reduce interface complexity,
- spare part inventory.

RAM analysis tools will be useful in supporting design decisions aimed at reducing system down time.

B.3.1.2 Manufacture for Availability and Quality Management

A significant proportion of subsea failures, especially those occurring in early life, arise as a result of faults or defects introduced during manufacture, assembly or construction in an otherwise reliable product. Many of these faults and defects arise due to problems or errors in the manufacturing process. Where a manual procedure is part of the manufacturing process (e.g. manual welding, soldering or manual assembly), this may be related to human error. In other cases where manufacture and assembly is automated, failures may arise when there is an excursion outside the manufacturing process limits. In some cases this may also be related to the set up skills of a machine engineer. Manufacture to a high level of quality will, therefore, often require careful attention to human reliability and the skills and competence of the manufacturing work force.

It is critically important that the design reliability is not compromised during manufacture and assembly of subsea packages or during construction. Good manufacturing quality procedures combined with knowledge of failure mechanisms should be adopted to ensure delivery of design reliability. The manufacture of reliable equipment is strongly influenced by an organization's quality management systems and the implementation of quality control and continuous quality improvement activities during manufacture.

Quality control is intended to provide stability to the manufacturing process and to product performance. Aligning quality control in manufacture to reliability can result in the consistent delivery of reliability performance by controlling variability in material properties, geometric tolerances, surface finish conditions and preventing unwanted deviations from standard performance indicators.

Quality control procedures usually involve the measurement of specific manufacturing metrics to ensure that the process stays within specified performance limits and that the product conforms to requirements. A key element is the detection of any non-conformances and excursions beyond manufacturing limits likely to reduce reliability. To this end careful consideration should be given to the methods of identifying non-conformances and manufacturing deviations. Various testing procedures and methods are routinely used, including:

- FAT,
- HASS,
- screening (100 % product testing) or monitoring (sample testing),
- seal integrity (leak tests),
- SIT,
- statistical process control.

It should be noted that function or performance tests do not necessarily relate to reliability performance. A device which passes a single function test does not imply that it is reliable, as a level of reliability will require testing over a number of tests or time in an environment which simulates, or exceeds, that expected in practical operation.

Quality improvement is the process of introducing value added change to a product. This should be reflected in manufacture for reliability as a reduction of material property variation. Note that improvements in quality should be reflected in design for reliability and may require alterations to the quality control test methods and acceptance criteria. Many manufacturing or quality practices may be implemented to initiate value-added reliability improvements, these include:

- burn-in,
- ESS,
- HALT,
- HASS,
- PFMEA,
- material properties,
- thermal cycling,
- tooling tolerances.

NOTE Many test techniques such as HASS, FAT, pressure testing and leak testing, etc. are both methods for revealing defects, quality control and for improving reliability if they are combined with fault correction or removal of defective items when found.

The output from this process is closely linked with reliability assurance and reliability qualification and testing. However, this process also introduces an iterative loop into the design process. Any alterations to the design resulting from this process should be subject to a re-assessment.

B.4 Process 4—Reliability Assurance

B.4.1 Description

Reliability assurance is the process of collating, assessing to provide evidence of availability achievement and communicating this reliability information in a formal document. This information is generated during a field development project so that the end customer has the best possible indication at any stage during the project of the system's current and eventual technical effectiveness. Technical effectiveness includes a system's functional performance attribute and system availability attribute (which includes reliability, durability and maintainability).

The purpose of reliability assurance is to demonstrate that the availability requirements have been met and the extent to which the availability goals will be achieved. Reliability assurance is the essential element of managing technical risk as it is the process of identifying, assessing, justifying and, most importantly, communicating the information pertaining to risks to the technical effectiveness of the system.

The key output from the reliability assurance process is the RAD. The purpose of the RAD is to provide the customer with evidence of progressive achievement during the project. The RAD is a living document initiated at the feasibility stage of a project and is continually updated throughout the various project stages up to and including the operate stage.

Documented evidence provided in the RAD will vary in quality depending on its source. Table B.5 provides comments on the different data types available.

Table B.5—Types of Reliability Assurance Evidence

Evidence Type	Comments
Current Field Data	These are the most reliable data. However, the frequency with which data is received and the accuracy of the data collection method will influence the decision making process and the available action time [field data may be "dirty" (unreliable or incomplete)].
Test/Trial Data	Trial data can more closely replicate actual conditions in comparison to previous use data that has been modified.
Previous Use Data	These are possibly the most abundant data, especially for mature technology. However, close attention should be directed towards the relevance of the data (e.g. the ambient operating conditions) when making reliability predictions.
Simulations	These can provide useful insights that may have otherwise been overlooked. However, output generated is susceptible to model complexity and the quality of the input data.
Calculations	These can provide a high level indication of the target metrics but will not necessarily accommodate uncertainties relating to the input data.
Expert Opinion	Although these data are sometimes valuable, care should be taken when defending assertions based on these data alone as they may be subject to biases and flawed perceptions.

The RAD may comprise of a number of documents from a variety of sources but they should all include the following information indicated in Table B.6, which may be implemented as a guide to the construction of a RAD. The size of the document should be reflected in the sources and levels of project and technical uncertainty and/or risk.

The RAD should be tailored to reflect the required assurance and decision support at the different project stages. There may be two basic types of RADs created during a project; a system or project RAD and more detailed equipment RADs. A system or project RAD should provide a synopsis of the reliability effort and outputs to support project based decision making (e.g. continuation to the next project stage or selection of the preferred concept). Equipment RADs should be more detailed to support the claims of the availability performance; where appropriate, they should also reflect the accumulated assurance and continuous improvement of equipment over multiple projects throughout the equipment's life cycle. The RAD, therefore, becomes a living document both over the course of a project life cycle but also equipment's life cycle.

Table B.6—Suggested Constituent Parts of a Reliability Assurance Document (RAD)

System Description	Clear definition of the operating environment, system layout should be defined as part of preexisting project documentation and so can be references as an external document.
Availability Requirements	Include the availability goals and requirements defined for the equipment. Include any process or procedural requirements.
Strategy for Availability Achievement	Summarize the strategy implemented to achieve the project goals and requirements. Including and indication of the technical risk as defined by the technical risk categorization with justification of the category selected and an indication of the level of effort required.
Reliability Plan	The plan of reliability tasks defined to deliver the availability performance can be fed directly into (or referred in) the assurance document.
Availability Evidence	Present the summarized results of any reliability activities implemented as part of the project. The evidence provided should concisely support the contention of the technical effectiveness, including assurance that the requirements have been met and the extent to which the goals will be met. Table B.5 provides some guidance on the different types of evidence that may be generated. Comprehensive presentation of the results may be referred to in an annex.
Availability Claims	Any claims of the technical effectiveness made on the basis of the availability evidence should be included.
Limitations on Use	Some activities will have determined the operational envelop or operational conditions that prevent the confident delivery of the availability requirements. Any limits identified where the technical effectiveness cannot be adequately guaranteed should be included here.
Conclusions and Recommendations	Initial conclusions and recommendations for future reliability activities are specified here.
References	References to external documents.
Appendices	Include the bulk of the data generated during the project that is not referenced externally.

Copyright American Petroleum Institute
 Provided by IHS under license with API
 No reproduction or networking permitted without license from IHS

B.5 Process 5—Risk and Availability Analysis

B.5.1 Description

Risk and availability models and analyses provide reliability management support by identifying failure modes/logic and the frequency of occurrence. Some of the techniques are closely linked to setting availability goals and requirements.

Analysis of the risk and availability models can be either qualitative or quantitative; qualitative models are used for failure mode identification purposes, which can then be further analyzed with quantitative methods. The process of modeling and analysis is initiated by the qualitative determination of failure modes and continues through to quantitative importance analysis as indicated by the procedure outlined below:

- identify failure modes (qualitative),
- assess the probability of occurrence of each failure mode (quantitative),
- assess the consequence of failure (for a quantitative analysis this may be expressed in terms of a recovery cost),
- populate reliability/availability model with the relevant data,
- determine the reliability/availability and respective importance of each failure mode (quantitative risk = probability × consequence (cost), which may be interpreted as “expected” cost).

Analysis and models usually focus on function, hardware or process. The specific type of assessment will depend on the amount of information available (i.e. the project stage), the subject of the analysis and the source of technical risk (i.e. high technical risk category of the change risk factor) as shown in Table B.7. Where multiple “X” exist, there is either a combined focus (e.g. analysis associated with manufacture will consider processes and hardware) or the analysis subject will determine function, hardware or process.

- Functional assessments consider what an item is intended to achieve, without too much emphasis as to how it will be achieved. These types of analysis tend to occur during earlier project stages when decisions are more conceptual.
- Hardware assessments consider tangible items and address how or why something occurs. Hardware analysis can be performed once equipment has been identified.
- Process assessments review predefined sets of activities. These types of assessment can be performed once a working or operational procedures have been defined or in the assessment of organizational capability. Process assessments will often be of combined focus to consider the interaction with hardware and/or functions.

Table B.8 to Table B.17 outline some key risk analysis techniques. However, other techniques have been developed and can be used if appropriate.

Table B.7—Relationship of Analysis Type to Project Stage and Technical Risk Categorization

Project Life Cycle Stage	Function	Hardware	Process
Feasibility	X		
Concept Selection	X	X	
FEED	X	X	
Detailed Design	X	X	X
Manufacture		X	X
SIT/Installation/Commissioning		X	X
Operations—General		X	X
Operations—Intervention		X	X
Operations—Life Extension		X	X
Operations—Modification	X	X	X
Change Risk Factor			
Reliability	X	X	X
Technology	X	X	
Environment		X	
Architecture		X	
Organization	X		X

Table B.8—Failure Modes, Effects and Criticality Analysis (FMECA) Summary

Failure Modes, Effects and Criticality Analysis (FMECA)	
Objective	
1)	To identify all possible failure modes of a system, design or process.
2)	To identify all possible consequences of the failure modes.
3)	To prioritize areas of system, design or process improvement.
Timing of Application	
Due to the versatility of the process, a FMECA can be performed at any stage of a project. However, the focus of the analysis does change depending on when a FMECA is performed.	
1)	A functional FMECA is performed prior to the definition of specific hardware. The focus of attention is geared towards the functions that the hardware is expected to perform.
2)	A hardware FMECA is implemented once the hardware has been identified and the assessment can focus on the specific details of the systems/packages/components.
3)	A process FMECA is implemented for the specific assessment of the manufacturing procedures. The process FMECA is usually performed in terms of the process hardware.
Procedural Outline	
Reference: [1]	
1)	Define the system to be analyzed, including: internal and interface functions/hardware, performance expectations and definitions of failure.
2)	Construct a block diagram to represent functional/hardware inter-dependencies and inter-relationships.
3)	For each functional/hardware item and interface, identify all potential failure modes and their immediate effects on the function/hardware and system.
4)	For each failure mode, assign a severity category (1—catastrophic to 4—minor) based on a worst case consequence scenario.
5)	For each failure mode, assign a probability of occurrence level or criticality number.
6)	Plot the failure modes on a criticality matrix.
7)	For each failure mode, identify detection methods and compensating provisions.
8)	Identify corrective actions (design or otherwise) required to remove or mitigate the risk and assess the effects of the corrective actions.
9)	Agree and log the corrective actions required to manage failure mode risk.
Data Requirements	
1)	Full system definition.
2)	Failure consequence input.
3)	Failure probability input.
Strengths	
1)	Applicable at all project stages.
2)	Versatile—applicable to high level systems, components and processes.
3)	Can prioritize areas of design weakness.
4)	Systematic identification of all failure modes.
Weaknesses	
1)	Does not identify the root cause of the failure mode.
2)	Can be a time consuming task.

Table B.9—Fault Tree Analysis (FTA) Summary

Fault Tree Analysis (FTA)	
Objective	
1)	To logically represent all the possible failure modes of a system or package.
2)	To identify the technical cause of the specified unwanted event.
3)	To identify the minimum cut sets of a given system/package/component.
4)	To estimate/predict the system reliability performance.
Timing of Application	
1)	Fault tree construction is best applied to specific packages or systems during front end engineering design (FEED) or detail design.
2)	The fault tree should grow as the design detail increases throughout the project.
3)	FTA may be required as part of and to support a FMECA, e.g. to identify system failure modes and mechanisms.
4)	FTA can also be conducted to help understand failures should they be observed during operations.
Procedural Outline	
Reference: [2]	
1)	Define the scope of the analysis, including: the definition of the system, the agreed level of analysis detail and any assumptions made.
2)	Identify the top event as the focus of the analysis.
3)	Identify the immediate, necessary and sufficient causes of the top event.
4)	The relationship between the immediate causes and the top event is represented by a logic gate (common logic gates are OR, AND).
5)	Treat each immediate cause identified in Step 3 as a subtop event. For each subtop event, identify the immediate necessary and sufficient causes.
6)	Repeat Step 3 and Step 4 until the basic unit/event is identified. The basic unit/event is the point at which the analysis can add no further value.
7)	Logical assessment of the tree implements Boolean reduction, which is best resolved by implementing software packages for complex systems.
Input Data Requirements	
1)	Tree construction requires an intimate knowledge of the system logic.
2)	Numerical analysis requires reliability parameters (e.g. hazard rate or Weibull reliability parameters) for each of the basic units/events.
Strengths	
1)	Can support common cause failure analysis.
2)	Can predict the probability of occurrence of a specific event.
3)	Can support root cause analysis (RCA).
4)	Compatible with event trees for cause—consequence analysis.
5)	Supports Importance analysis and Monte Carlo simulation (MCS).
Weaknesses	
1)	Complex systems may become difficult to manage and resolve manually.
2)	Not suited to the consideration of sequential events.

Table B.10—Reliability Block Diagram (RBD) Summary

Reliability Block Diagram (RBD)	
Objective	
1)	To provide graphical representation of a system's reliability logic.
2)	To give a simplistic view of system fault tolerance.
3)	To predict the system reliability.
Timing of Application	
1)	A top level RBD can be constructed as soon as a system layout has been defined.
2)	More detailed RBDs can be nested within the top level RBD as the design detail develops.
3)	An RBD may be required whenever a design failure modes, effects and criticality analysis (FMECA) is performed.
Procedural Outline	Reference: [3] [5]
1)	Define a state of system success.
2)	Divide the system into equipment blocks that reflect the logical behavior of the system such that each block is statistically independent and as large as possible.
3)	Define a start node and end node(s).
4)	Construct an RBD such that the blocks are connected according to a success path from the start node to end node(s). A success path indicates the arrangement of blocks that must exist in the working state to observe the defined state of system success [i.e. transition from the start node to the end node(s)]. Likewise, failure of a block will partially or completely prevent transition from start node to end node(s) depending on the system reliability logic.
5)	When constructing a diagram, ensure not to repeat blocks (unless the system observes redundant capability).
6)	Note that system reliability logic may not be the same as the system function logic. Typically, RBD will be composed of series or parallel blocks. However, in some systems, failure logic requires an RBD comprised of bridge or star networks, which require special techniques to solve.
7)	As the design evolves, each block can be broken down into smaller blocks and a more detailed RBD created. These more detailed RBDs can be nested within the higher level RBD blocks, as long as the logic allows it.
8)	Logical or numerical assessment of the RBD is best implemented through software.
Input Data Requirements	
1)	Thorough knowledge of how the system operates.
2)	Reliability parameters (e.g. hazard rate or Weibull reliability parameters), for each block in the diagram, relevant to the expected conditions.
Strengths	
1)	The best method of graphically representing complex system logic.
2)	Good visualization of redundant system logic.
3)	Supports importance analysis and assessment through Monte Carlo simulation (MCS).
4)	Good precursor to all other analysis methods.
Weaknesses	
1)	Construction of RBD can be difficult for complex systems.
2)	Numerical assessment of the RBD can be very time consuming (if performed manually or if multiple nested RBDs are apparent).
3)	Becomes very data intensive when there are more detailed levels.
4)	May require multiple RBDs for multiple functional modes.

Table B.11—Event Tree Analysis (ETA) Summary

Event Tree Analysis (ETA)	
Objective	
1)	To graphically describe how failure events propagate through a system.
2)	To determine the probable consequences of specified failure events.
3)	To identify areas requiring risk mitigation.
Timing of Application	
1)	Apply prior to the completion of system/subsystem design within front end engineering design (FEED) and detailed design to allow for appropriate mitigations to be designed into the system.
2)	Can be applied to support any decision making process.
3)	May be required whenever a failure modes, effects and criticality analysis (FMECA) is undertaken.
Procedural Outline	
Reference: [6]	
1)	Define the scope of the analysis, including: the definition of the system, the agreed level of analysis detail and any assumptions made.
2)	Identify the initiating event to be assessed.
3)	Identify all credible and immediate outcomes from the initiating event, the probability with which they occur and their consequences.
4)	Treat each immediate outcome identified in Step 3 as a subinitiating event. For each subinitiating event identify all the credible and immediate outcomes from the subinitiating event, the probability with which they occur and their consequences.
5)	Repeat Step 4 until the final outcomes are identified. A final outcome is a resultant event for which no further immediate outcomes can be identified within the scope of the assessment.
6)	The numerical assessment of the event tree considers the cumulative expected consequence of each branched path defined. This is best implemented with software support.
7)	Identify and recommend appropriate mitigations, review the event tree with these mitigations in place.
Input Data Requirements	
1)	Probability of each branched event. This may require reliability parameters (e.g. hazard rate or Weibull reliability parameters).
2)	Consequence of each branched event.
Strengths	
1)	Integration with decision trees.
2)	Compatible with fault trees for cause—consequence assessment.
3)	Simple approach.
4)	Good at assessing sequential events.
5)	Supports the consequence assessment of FMECA.
6)	Supports Monte Carlo analysis.
Weaknesses	
1)	Tree can become very large and difficult to manage for complicated event sequences or for systems with large numbers of components.
2)	May not be capable of representing feedback loops.
3)	Requires thorough knowledge of the propagation of events through the system.

Table B.12—Physics of Failure Summary

Physics of Failure	
Objective	
1)	Predict the reliability of designs for which prototypes cannot be built.
2)	Predict the reliability of designs for which qualification tests cannot be run.
3)	Reduce testing time during product research and development (R&D).
Timing of Application	
1)	Best used during the early stages of R&D of new technology.
2)	Can be used during detailed design to understand uncertainty and determine required tests.
Procedural Outline	Reference: [7]
1)	Define the scope of the analysis, including the system definition and the level of detail required.
2)	Identify the failure mechanism for which the assessment is required [e.g. by fault tree analysis (FTA)].
3)	Model the failure mechanism in terms of the fundamental mechanical, electrical, thermal and/or chemical processes.
4)	Determine the statistical distributions of each design parameter (e.g. material properties, operational stresses, etc.).
5)	Calculate the probability of failure either by numerical integration, Monte Carlo simulation (MCS) or approximation methods. Typically, physics of failure analysis is implemented using a combination of techniques such as event trees and stress strength interference. These are best implemented with software support.
6)	Identify and recommend appropriate design improvements and/or test regimes, review the model with the appropriate data.
Input Data Requirements	
1)	Statistical distributions of all relevant material properties.
2)	Statistical distributions of all relevant operational stresses.
Strengths	
1)	Particularly useful when material and operational load properties are well defined.
2)	Useful when the failure mechanism can be represented by well defined and fundamental physical, electrical, thermal and/or chemical processes.
3)	Supported by Monte Carlo methods.
4)	Can reduce the required reliability growth testing cycle.
Weaknesses	
1)	Very data intensive.
2)	Cannot be implemented if the failure mechanism is not fully understood.
3)	Does not consider nontechnical failure mechanisms.

Table B.13—Importance Analysis Summary

Importance Analysis	
Objective	
1)	To establish the effects of the modeling assumptions.
2)	To establish the effect of parameter uncertainty.
3)	To identify the sensitivity of model output to reliability input data.
Timing of Application	
1)	Importance analysis is best applied when setting availability goals and requirements.
2)	Importance analysis can be applied when it is necessary to identify where attention should be focused.
Procedural Outline	Reference: [8] [9] [10] [11]
There is no standard procedure for importance analysis. In most cases the importance analysis occurs after one of the other modeling procedures [often, fault tree analysis (FTA) or Monte Carlo simulation (MCS)]. Typical importance techniques in reliability engineering do not consider the availability of a system so may be of limited utility, the following are all supported by reliability software packages.	
1)	The Fussell-Vesely importance of a component is the conditional probability that the component has failed given that system failure has occurred.
2)	The Barlow-Proschan importance of a component is the average number of system failures up to a specified time caused by the component failure.
3)	The Birnbaum importance of a component is the probability that component failure causes system failure.
Input Data Requirements	
1)	Importance analysis will require all those data necessary for the modeling/analysis technique to which the importance analysis is to be applied.
2)	MCS based importance measures will require all those data inputted to the simulation.
Strengths	
1)	Helps prioritize effort into the reduction of uncertainty or the improvement of reliability.
2)	Provides insight into the key uncertainties that are driving the (un)reliability.
3)	Basic ranking concept can be applied to define case specific importance measures.
Weaknesses	
1)	Importance analysis determined via simulation can become time consuming.
2)	Each of the reliability measures has its own limitations.
3)	May not rank importance based on availability.

Table B.14—Qualitative Common Cause Failure Analysis Summary

Common Cause Failure Analysis (Qualitative)	
Objective	
1)	To identify those parts, components or packages that may experience (near) simultaneous failure due to a common event.
Timing of Application	
1)	Best used near the end of system/subsystem design to allow for appropriate mitigation.
2)	Can be applied whenever a failure modes, effects and criticality analysis (FMECA) or fault tree analysis (FTA) is performed.
Procedural Outline	Reference: [12]
1)	Define the scope of the analysis, including the system definition and the level of detail required.
2)	Prepare a list of credible common causes to which the system is exposed. A common cause is an event or mechanism that can cause two or more simultaneous failures.
3)	Identify the domain of each of the common causes. The domain is the area in/at which the common cause might occur/affect.
4)	Identify all of the system minimum cut sets (e.g. from FTA). A cut set is a group of parts/components/packages which when failed cause the system to fail. A minimum cut set occurs if, when one failed part/component/package is restored, the system returns to the operational state.
5)	For each component within a minimum cut set, list all of the failure events that could occur as a result of each common cause event.
6)	Identify if the failure events in each minimum cut set could occur as a result of, and are in the domain of, the common cause event.
Input Data Requirements	
1)	Complete definition of the system.
2)	Complete understanding of the part/component/package history (i.e. all those events that link two or more components).
Strengths	
1)	Identifies candidates of common cause failure.
2)	Becomes an extension of other analysis techniques.
3)	Reliability data is not required.
4)	Particularly useful when considering systems with active redundancy.
Weaknesses	
1)	Needs the definition of all minimum cut sets—can lead to long assessment time for complex systems.
2)	Link to root cause analysis (RCA) may get overlooked.

Table B.15—Quantitative Common Cause Failure Analysis Summary

Common Cause Failure Analysis (Quantitative)	
Objective	
1)	Predict/approximate the probability of (near) simultaneous failure of two or more parts, components or packages due to a common event.
2)	Determine the required reliability of certain barriers to common cause events.
Timing of Application	
1)	Best used near the end of system/subsystem design to allow for appropriate mitigation.
2)	Can be applied when any systems reliability analysis is performed.
Procedural Outline Reference: [12]	
Numerous methods are available for the quantitative assessment of common cause failures. Data availability determines the detail to which the assessment can be performed. When conditional probabilities are known/accurately estimated, the parametric method can be used:	
1)	If the conditional probability of a minimum cut set occurring as a result of a common cause event given that the common cause event has occurred, is known as $P[M X]$, then the probability of occurrence of the minimum cut set as a result of the common cause event, $P[M']$, is: $P[M'] = P[X] P[M X]$ Where $P[X]$ is the probability of occurrence of the common cause event. This is especially applicable for setting some reliability requirements when $P[M X] = 1$ and $P[X]$ is a controllable barrier (e.g. failure of subsea electronics given failure of a seal). If the data required for the parametric assessment cannot be credibly attained or estimated then an approximation method should be used. These are based on expert judgment of the strength of the statistical dependency of the simultaneous failure as a result of the common cause event.
2)	The lower bound method should be implemented when the dependencies between the failure events and the common cause event are thought to be weak, yet the probability of each independent failure event is known. The lower bound approximation of the probability of failure of the minimum cut set, $P_{LB}[M]$, as a result of the common cause failure is: $P_{LB}[M] = P[E1]P[E2], \dots P[En].$ Where $P[En]$ is the probability of the nth failure event in the minimum cut set.
3)	The upper bound method should be implemented when the dependencies between the failure events and the common cause event are thought to be strong, yet the probability of each independent failure event is known. The upper bound approximation of the probability of failure of the minimum cut set, $P_{UB}[M]$, as a result of the common cause failure is: $P_{UB}[M] = \min\{P[E1], P[E2], \dots, P[En]\}.$ Where $P[En]$ is the probability of the nth failure event in the minimum cut set.
4)	The square root method should be implemented when dependencies between the failure events and the common cause event are not strong or weak, yet the probability of each independent failure is known. The square root approximation of the probability of failure of the minimum cut set, $P_{SR}[M]$, as a result of the common cause failure is: $P_{SR}[M] = \{P[M]LBP[M]UB\}^{1/2}.$
Input Data Requirements	
1)	Failure data for each independent failure event in the minimum cut set.
2)	Expert opinion on dependencies.
Strengths	
1)	Approximation methods are simple techniques.
Weaknesses	
1)	Approximation methods may over/underestimate the probability of common cause failure.
2)	Parametric method is heavily reliant on valid data.

Table B.16—Reliability Availability Maintainability (RAM) Analysis Summary

Reliability Availability Maintainability (RAM) Analysis	
Objective	
1)	To evaluate the ability of the system to remain in the operational state.
2)	To support the definition of the maintenance or intervention support strategy.
3)	To represent the combined reliability analysis and modeling effort in operational terms.
Timing of Application	
1)	Best initiated as a high level RAM model during concept selection
2)	The RAM model can be updated throughout the project as the design detail increases.
3)	Can be implemented when defining operational and maintenance strategies.
Procedural Outline	Reference: [6] [9]
1)	Define the scope of the analysis, including the system definition, assumptions and the level of detail required.
2)	Clearly define the metrics by which the system is to be assessed and the methods by which they are calculated.
3)	Create a model that logically represents the system in terms of an reliability block diagram (RBD), event tree, fault tree or functional block diagram.
4)	Populate the model with input parameters for reliability, operations and maintenance strategies.
5)	Evaluate the model by deploying Monte Carlo simulation (MCS) methods to assess the nature of input parameter uncertainty on the defined metrics. This is best implemented with software support.
6)	Identify recommendations for operational performance improvements; this may be in terms of the intervention and sparing strategy or the need for reliability stretch.
7)	Review the model in terms of the recommendations suggested in Step 6.
Input Data Requirements	
1)	Reliability and maintainability (RM) input parameters for every component in the model.
2)	Asset operations, maintenance and intervention strategy.
3)	Production profile.
Strengths	
1)	Provides more operationally suitable performance metrics than system reliability analysis.
2)	Can consider multiple operational/failure modes—closest representation of the real system.
3)	Supports Monte Carlo methods.
4)	Closely linked to setting availability goals and requirements and reliability value analysis.
5)	Builds on the output from other reliability analysis techniques.
Weaknesses	
1)	Very data intensive.
2)	Potentially time consuming.
3)	May be based on invalid assumptions.

Table B.17—Root Cause Analysis (RCA) Summary

Root Cause Analysis (RCA)	
Objective	
1)	Resolve problems that affect system reliability.
2)	Identify the facts relating to the occurrence of a failure or event at root cause level. Ideally this will require human and organizational factors to be addressed in addition to technical root causes.
Timing of Application	
1)	RCA is implemented when a failure or near miss has been observed or to resolve possible frequent/recurring nuisance events.
Procedural Outline	Reference: [10]
1)	Report the event or incident upon observation. The incident report form should include sufficient information to support the decision for a full RCA. The information recorded should include a description of the event, when it occurred, what is the perceived cause and indication if the event qualifies for full RCA.
2)	Classify the event (typical categories might be: equipment damage/failure, operating performance, economic performance, safety, regulatory compliance) and decide if it qualifies for full RCA.
3)	Collect data—this may be achieved by interview, design review or application/maintenance review.
4)	Use the data collected to support the construction of a fault tree to identify the root cause or an event tree to determine the sequence of events that lead to the event/incident. Determine potential root causes.
5)	Validate the root causes identified (e.g. by testing) and the assumptions made during the analysis. If the root cause is not valid, then Step 3 and Step 4 should be reviewed and the activities revised where necessary.
6)	Report root causes and propose potential corrective actions.
7)	Assess the value addition of the proposed corrective actions and select the preferred solution.
8)	Agree and log the corrective actions required to manage the root cause.
Input Data Requirements	
RCA is grounded on the collection of sufficient information to isolate the fundamental cause of the event reported. As a result, the input data requirements are failure specific. The quality of RCA depends on the expertise, knowledge and experience of the analysts.	
1)	The initial incident reporting should include a thorough event description comprising: the failure mode, when it occurred, the conditions leading up to failure, the probable cause, the immediate corrective actions and the immediate consequences.
2)	The data requirements of the supporting techniques [e.g. fault tree analysis (FTA) and event tree analysis (ETA)].
Strengths	
1)	Relates equipment failure to the 12 key processes (KPs).
2)	Driven by a number of reliability techniques.
3)	Logical investigation procedure.
4)	Drives a formal data collection methodology.
5)	May support common cause failure analysis.
Weaknesses	
1)	Can be resource intensive.
2)	Improper application may isolate the wrong root cause or not isolate the true root cause.

B.6 Process 6—Verification and Validation

Table B.18 indicates the verification/validation activities required for each of the KPs. The importance and required effort of this key task increases with the associated level of risk. All processes and tasks should be verified to ensure that they have been implemented correctly.

Table B.18—Recommended Verification and Validation of the Key Processes (KPs)

Key Process	Verification	Validation
Technical Risk Categorization	X	
1) Definition of Availability Goals and Requirements		
Reliability Value Analysis	X	X
Define Availability Requirements	X	X
2) Organizing and Planning for Availability		
Organizing for Availability	X	
Planning for Availability	X	
3) Design and Manufacture for Availability	X	X
4) Reliability Assurance	X	
5) Risk and Availability Analysis	X	X
6) Reliability Qualification and Testing	X	X
7) Project Risk Management	X	
8) Performance Tracking and Data Management	X	X
9) Supply Chain Management	X	
10) Management of Change	X	
11) Organizational Learning	X	

The verification and validation process is complementary to the other KPs within the availability strategy as it serves to check the application of all processes/tasks/activities. It is an important process, therefore, when considering the confidence and value of the evidence presented within the reliability assurance documentation.

Verification and validation are best conducted via peer review independent of the project delivery team. Note that this does not necessarily mean that the validation and/or verification authority should be an external organization. During the organization and planning for availability, the validation/verification authority should be identified for each of the KPs.

B.6.1 Verification

Verification is the process of determining if a technique or activity has been performed and/or completed but also the extent to which it conforms to internal or global standards of application or operation. It specifically addresses the question, “Are the reliability activities being implemented correctly?” Verification should be applied to all KPs and associated tasks to confirm that they have been implemented in accordance with the plans and customer goals and requirements.

- Validation is the process used to ascertain the appropriateness of data, assumptions or techniques in terms of the objectives of both the availability strategy and individual availability activities. It specifically addresses the question, “Are the correct reliability activities being implemented?”
- Validation should consider the applicability of historical availability data used for modeling and analysis in terms of the expected environmental conditions and area of application.
- Models should be validated to ensure that the predicted results adequately reflect reality.
- Tests should be validated such that they generate the desired type of output (e.g. functional tests do not necessarily demonstrate reliability).

- Design and manufacture for availability:
 - Are suitable reliability improvement techniques being implemented?
 - Are appropriate maintainability designs theories being considered?
- Reliability qualification and testing:
 - Is the correct test being specified given the desired results of the test?
- Performance tracking and data management:
 - Are suitable data elicitation techniques being applied?
 - Is data being stored and handled correctly?
- Availability analysis/reliability value analysis:
 - Is the correct analysis tool being implemented given the required results?
 - Is the model being populated with the right data?

B.7 Process 7—Project Risk Management

B.7.1 Description

All field developments are created in a project environment and involve risk. These risks should be managed and reduced to an acceptable level if the project is to be a success. While there are many areas of risk that are relevant to projects, the traditional dimensions of subsea project risk management are schedule, cost and safety.

The primary reason for including project risk management as a key reliability process facilitates the balance between the key project drivers, namely; reliability, cost and schedule. For example, actions taken to reduce CAPEX and time to first oil/gas may adversely impact on OPEX. Likewise, over-expenditure of effort to improve reliability may not yield overall value if CAPEX cost increases outweigh the benefits of reduced OPEX.

NOTE Here CAPEX is taken to mean the overall cost of design, engineering, procurement, manufacture, test, installation and commissioning, including reliability costs and OPEX is taken as the overall cost of operating and maintaining the system.

A balanced approach is needed. While project costs and schedules should be very carefully managed in most projects, realization of faults and reliability problems late in the design process will lead to more rapid escalation of correction/rectification costs than those found early in the project. This illustrates the important principle of front loading the design effort to identify, assess and act on potential system and package failure modes at the earliest possible time in the project.

There are a variety of project risk assessment methods, with varying degrees of complexity. Two levels of project risk assessment are recommended here;

- formal project risk analysis,
- risk review.

B.7.1.1 Formal Project Risk Analysis

A good project risk management methodology enables the project team to assess the impact of reliability activities on project risk during development. Typically this might involve the following stages:

- reliability task analysis,
- identification of project risk and consequences,
- risk—response analysis.

The first step is to list all the reliability tasks to be performed that are known at that time. The next step is to identify and list the risks that the task creates for the project and then to assign a category to each risk. Typical project risk categories include:

- cost,
- schedule,
- safety,
- supply chain.

Once the risks have been identified, appropriate responses can be developed and actions assigned.

B.7.1.2 Risk Review

The project risk review should be undertaken at the start of each project stage to support the technology risk categorization and planning tasks. The purpose of project risk management is to identify and assess the risks to the identified project activities. Of key relevance to the reliability achievement is the recognition of project risks that could impact on reliability (e.g. due to pressures on schedule and budget). Project risk reviews should be considered a component of good project management practice; reference should be made to the relevant in house documentation. Alternatively, reference should be made to IEC 62198:2001 [17] for guidance on the application of project risk management.

B.8 Process 8—Reliability Qualification and Testing

B.8.1 General

Exploitation of new technology in subsea field development projects or the use of existing technology in new environments is increasingly common. Particular attention should be given to qualification of these technologies to ensure that they are fit for purpose and meet project performance requirements. Existing industry standards (e.g. API 17D, Appendix F) should be regarded as a minimum, to be confirmed by a risk assessment process such as this or that detailed in API 17Q.

Qualification is the process by which systems are examined and evidence is provided to demonstrate that the technology employed meets the specified requirements for the intended use. The qualification process in some projects may start as early as feasibility if it is known that a specific piece of unqualified hardware will be required to exploit a field.

Technology development projects involve taking ideas and developing the technology to a level at which it can be applied in a field development. This section describes how new technology can be introduced to a field development project and how the readiness for use of a new technology can evolve in a product development project. While the basic philosophy is the same in both types of project, the timescale and degree of acceptable risk can differ in each.

It is generally found that as the product evolves through the various stages of product development, the uncertainties on the required performance decreases.

Theoretically, qualification is achieved when the uncertainty in the metric (performance) has reduced enough that the acceptance percentile (probability of achieving the performance requirement) crosses the target level for the required metric.

The objectives of the technology qualification process are:

- 1) provide a structured methodology for managing risk of failure in technology development projects and field development projects,
- 2) demonstrate the extent to which new technology is ready for use in a project,
- 3) demonstrate the extent to which existing technology is ready for use in new applications or under extended operating conditions,
- 4) increase confidence in the achievement of functional and performance requirements when new technology is applied in projects.

An item that incorporates new or novel technology requires a degree of proof that it is ready for use in a project. This proof is achieved through a qualification process. The qualification process is based on good engineering and technical risk management practices.

B.8.2 Technical Risk Management in Product Qualification

Systems incorporating new technology or using existing technology in new environments constitute greater risk to the operator in terms of uncertainty associated with reliability and availability performance. These risks should be carefully managed during development projects to achieve a robust and reliable product. The level of effort required to reduce the risk depends on the extent to which a given technology is “ready” for use in a particular application and the preparedness of the operator to implement appropriate qualification procedures for such applications.

The main principles are as follows.

- 1) A systematic technical risk assessment and risk management approach should be adopted, including:
 - a) definition of technology requirements (includes risk and reliability requirements),
 - b) identification of technology failure modes and mechanisms,
 - c) assessment of failure criticality (risk consequences) to determine relevance,
 - d) actions taken to reduce risk and uncertainties associated with:
 - i) technology itself (internal),
 - ii) operating characteristics and environment (external).
- 2) Proportionate qualification effort: The level of effort should be commensurate with the level of uncertainty associated with the operating regime, the environment, technology performance, and failure criticality.
 - a) A greater uncertainty in the operating environment or the performance of the new technology device will require a higher margin against failure, more robust qualification methods, and a greater weight of evidence of performance achievement.
 - b) The greater the consequence of failure, the greater the required confidence of reliable performance for the application and the greater the level of effort required in qualification.

B.8.3 Testing to Demonstrate Functional Performance

In the oil and gas sector, functional testing is the most common approach. The functional test logic is illustrated in Figure B.2. However, this form of testing has limited impact on reliability improvement. Sometimes the test method is predefined in a standard (e.g. an API standard) or it may be a company standard. To be of most benefit to the qualification of a product, the design of the test program should be based on a detailed understanding of the failure mechanisms expected for the operating conditions to which the product will be exposed.

B.8.4 Technology Readiness Level (TRL)

One assessment method which can be used to underpin the qualification process is the TRL which indicates the extent to which an item is “ready for use” given specified qualification factors/requirements.

The concept of TRL used to determine the qualification requirements has been adapted from work performed by the Seafloor Processing Community.

TRL indicates how far the processes in a technology qualification program for a particular technology have progressed. It can only be used with reference to a specific set of operating regime parameters and environmental conditions. If the operating regime or the planned environment changes, then the TRL may be downgraded for more demanding conditions or upgraded for less demanding conditions.

Eight TRLs have been defined ranging from minimum of 0, corresponding to an unproven idea, to a maximum of 7, corresponding to proven technology (installed and operating in the relevant conditions). These are shown in Table B.19.

The gap between the initial TRL and the required TRL will generally determine the qualification effort required within a project. The initial TRL is the qualification status of the equipment when it is first introduced to a project whereas the required TRL is the qualification status required for entrance into operations. Both initial and required TRLs should be

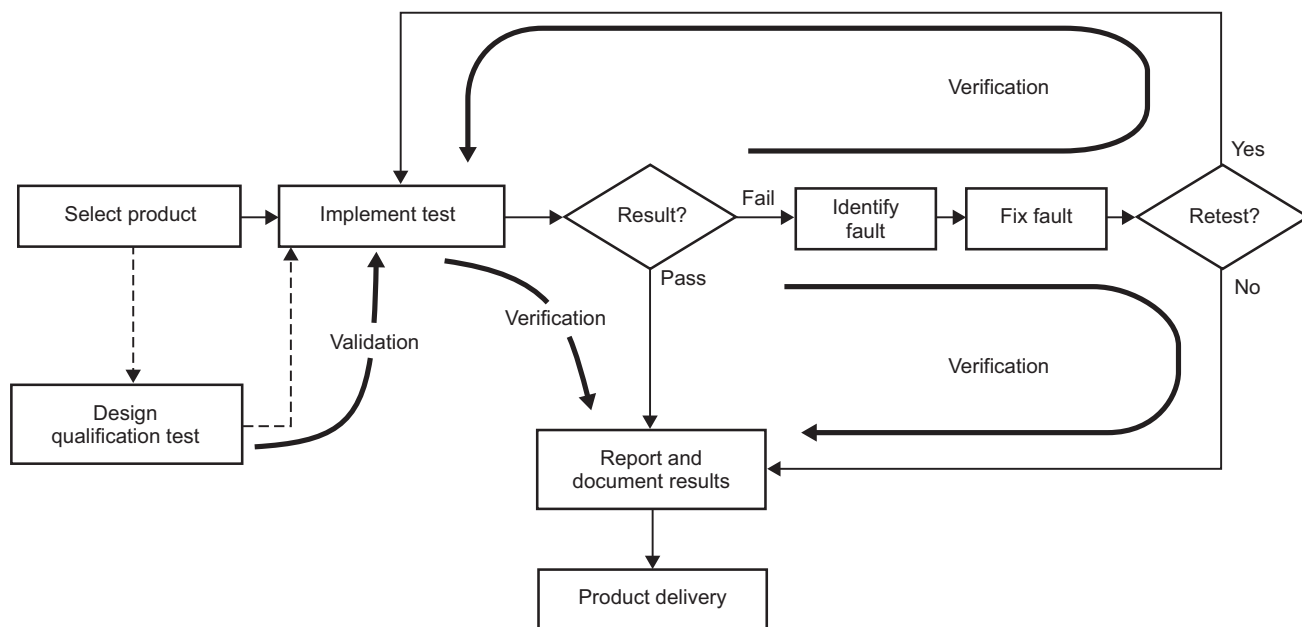


Figure B.2—Functional Test Logic

determined for a given project. In order for an item to be assigned a particular TRL, all the required function and performance activities and tests, as described in the TRL definition, are to be completed.

For example, for an item to have an initial TRL of 3 (TRL 3), it should have already completed all prototype function, performance and reliability tests required of TRL 3 and be ready to start environment testing to achieve TRL 4.

NOTE TRL assessment is relative to intended application. Equipment previously qualified on a previously installed project, will have a TRL 6, but only if the new application is similar in all key performance parameters. If, for example, the new application involves service at a higher pressure, then TRL 3 for the new application (i.e. the technology has been proven, but not in the intended environment; although the product will have been system integrated and installed, this will only be relevant after environmental performance is proven and the design remains unchanged).

Equipment TRL can be determined with input from the following KPs.

- Organizational learning—A review of lessons learned from previous projects can determine if a specific package has field life history (defines TRL 5) with relevant ambient stresses (defines TRL 6 or TRL 7 depending on operational lifetime).
- Data management—The existence of appropriate field data for the package (defines TRL 5) in the relevant ambient stresses (defines TRL 6 or TRL 7 depending on operational lifetime).

Planning for qualification should start as early as practicable. An early appreciation of qualification activities is especially important where there is a significant gap between the initial TRL and the required technology readiness level (required TRL).

The primary relationship between the qualification process and technical risk management is the effect of the level of qualification effort on project scheduling. The qualification plan should be aligned with the reliability plan (as there are common tasks) and adequately scheduled within the project plan so as not to erode project value.

Table B.19—Definition of Technology Readiness Levels (TRLs)

	TRL	Development Stage Completed	Definition of Development Stage
Concept	0	Unproven Concept (Basic R&D, paper concept)	Basic scientific/engineering principles observed and reported; paper concept; no analysis or testing completed; no design history
Proof of Concept	1	Proven Concept (Proof of concept as a paper study or R&D experiments)	a) Technology concept and/or application formulated b) Concept and functionality proven by analysis or reference to features common with/to existing technology No design history; essentially a paper study not involving physical models but may include R&D experimentation
	2	Validated Concept Experimental proof of concept using physical model tests	Concept design or novel features of design is validated by a physical model, a system mock up or dummy and functionally tested in a laboratory environment; no design history; no environmental tests; materials testing and reliability testing is performed on key parts or components in a testing laboratory prior to prototype construction
Prototype	3	Prototype Tested (System function, performance and reliability tested)	a) Item prototype is built and put through (generic) functional and performance tests; reliability tests are performed including; reliability growth tests, accelerated life tests and robust design development test program in relevant laboratory testing environments; tests are carried out without integration into a broader system b) The extent to which application requirements are met are assessed and potential benefits and risks are demonstrated
	4	Environment Tested (Pre-production system environment tested)	Meets all requirements of TRL 3; designed and built as production unit (or full scale prototype) and put through its qualification program in simulated environment (e.g. hyperbaric chamber to simulate pressure) or actual intended environment (e.g. subsea environment) but not installed or operating; reliability testing limited to demonstrating that prototype function and performance criteria can be met in the intended operating condition and external environment
	5	System Tested (Production system interface tested)	Meets all the requirements of TRL 4; designed and built as production unit (or full scale prototype) and integrated into intended operating system with full interface and functional test but outside the intended field environment
Field Qualified	6	System Installed (Production system installed and tested)	Meets all the requirements of TRL 5; production unit (or full scale prototype) built and integrated into the intended operating system; full interface and function test program performed in the intended (or closely simulated) environment and operated for less than 3 years; at TRL 6 new technology equipment might require additional support for the first 12 to 18 months
	7	Field Proven (Production system field proven)	Production unit integrated into intended operating system, installed and operating for more than three years with acceptable reliability, demonstrating low risk of early life failures in the field

In most field development projects, qualification activities will become most intense during FEED, detail design and manufacture when packages, components and parts to be used are defined along with their functional and reliability requirements.

It is important to recognize that package risk category is not the same as TRL. They are, however, related concepts and qualification activities will generally confirm the technical risk. Low technology risk projects by definition involve the implementation of field proven technology and as such the required TRL is 7. Similarly, it is not possible for novel technology (technology risk) to be field proven and so the highest TRL that the package can require is 6.

Note that this means that any given package can have multiple TRLs depending on the required application and may be comprised of components with differing TRLs. For example, a gate valve that has a sufficient proven track record within a certain ambient environment and with a specific duty cycle will have TRL 7. Placing the same hardware in a different operational environment and subject to, say, a different maintenance policy will alter the environmental stress as well as the duty cycle; this may result in a reduced TRL depending on the effect of the change in the stresses. To determine if the changes in stresses have altered the TRL, risk/reliability models should be constructed and analyzed; physics of failure models may be particularly useful to determine the effect of the altered stresses on the reliability.

If hardware exhibits a TRL less than the specified requirement then a qualification testing procedure should be defined to raise it to the required level. Qualification testing provides a physical examination of any materials or equipment that is intended for use during a subsea project. The output generated is fundamental to the reliability assurance documentation as this represents the generation of the highest quality data aside from current field data.

B.8.5 Outline Qualification Process Using TRL

Qualification testing can also provide a means of verification and validation of some of the risk and reliability modeling and analysis activities. Within the qualification process, there are three main purposes of testing:

- testing to demonstrate functional requirement,
- testing to screen out faults and manufacturing/assembly defects,
- testing to improve robustness and reliability.

An outline qualification process is shown below in Figure B.3. This incorporates appropriate TRL analysis and also the use of appropriate key reliability processes.

B.8.6 Use of Test Data to Estimate Reliability

For novel equipment or existing equipment to be used in new environments, historical field data will not be available as evidence of reliability achievement. In such cases, life testing of equipment provides an important alternative source of evidence of reliability achievement if the test conditions are equivalent to those in operation. It must be noted that the results of this testing may only apply to the inherent design reliability, which may be affected, by production and manufacturing processes, and ultimate use conditions. Failure test data can be statistically analyzed to estimate the failure rate of the component. The input data generally takes the form of a ranked list of times (cycles, etc.) to failure of a number of identical components. Repeat tests on the same component may be applicable if, after repair, it is as good as new. Annex D provides examples for calculating estimated failure distribution or estimating failure rate, based on performance verification test data. Examples of relevant standards for statistical analysis of data are outlined below.

B.8.6.1 Goodness of Fit Test

A goodness of fit test is generally required to test the assumption that an item's failures follow a specific failure pattern. This test usually has a minimum required number of failure observations. See Table B.20.

Table B.20—Standard Reference for Goodness of Fit Test

Reliability Model Assumption	Standard Reference
Constant failure rate or intensity	IEC 60605-6. Reference [13]
Weibull	IEC 61649. Reference [14]
Power law (repaired items)	IEC 61710. Reference [15]
Reliability growth	IEC 61164. Reference [16]

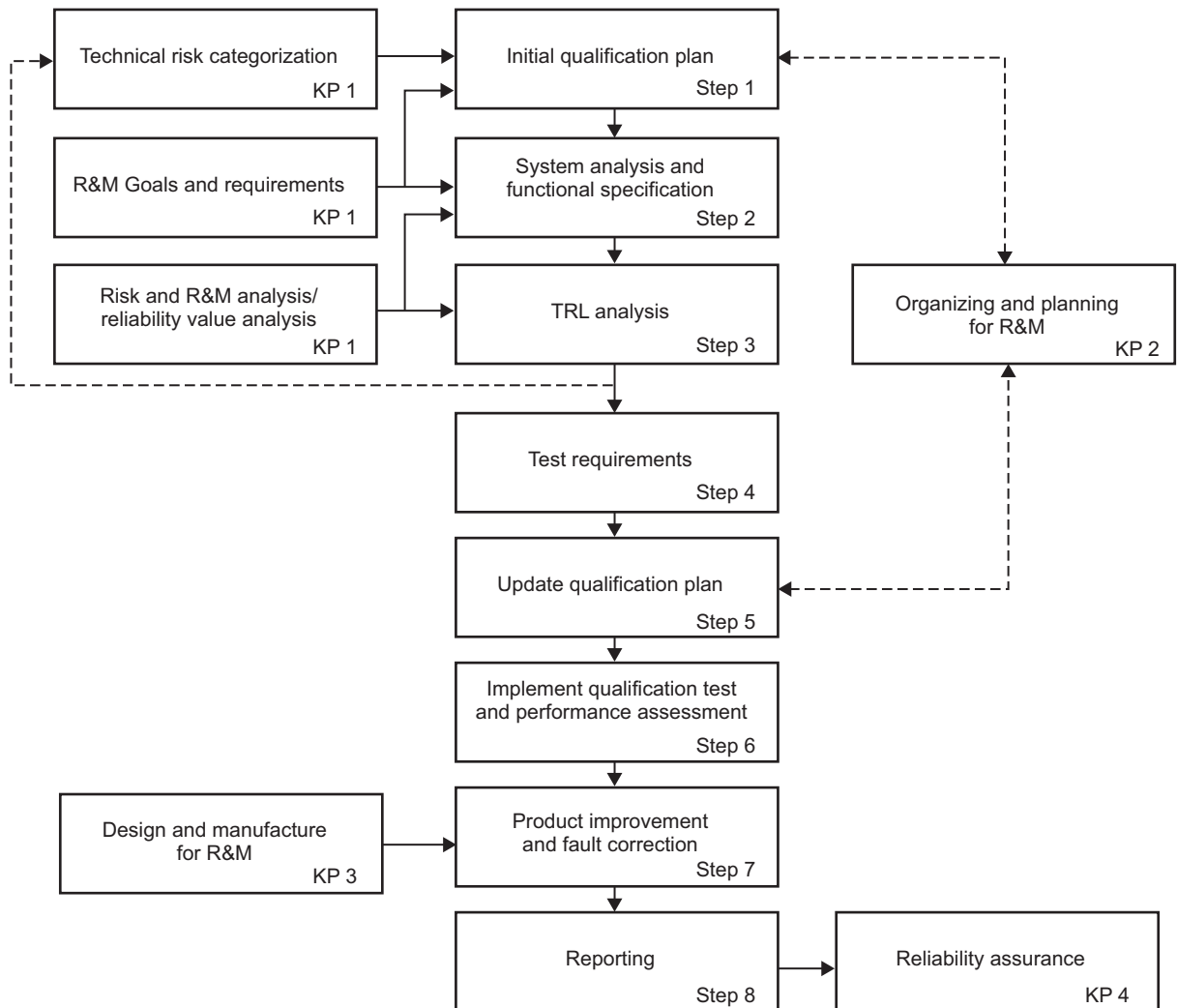


Figure B.3—Outline Qualification Process

B.8.6.2 Estimating Reliability Performance

The reliability of an item may be estimated from test data. These analytical methods generally start by assuming a distribution applies and then a fit is made to the assumed distribution to determine the statistical parameters of the distribution (a goodness of fit should be included with this estimate). The statistical parameters can then be used to estimate the reliability or probability of failure of the item. In most cases it will be necessary to test a number of distributions. Selection of the distribution can be based on either the best fitting distribution or a preferred/most convenient distribution. For example, a best fit may suggest use of a Weibull distribution with a non unity β value but the analyst may prefer to use the best fit to an exponential distribution to achieve consistency with other data or with a reliability specification to achieve a particular failure rate.

Table B.21—Standard Reference for Reliability Parameter Estimates

Reliability Model Assumption	Standard Reference
Exponential	IEC 60605-6. Reference [13]
Weibull	IEC 61649. Reference [14]
Power law (repaired items)	IEC 61710. Reference [15]
Reliability growth	IEC 61164. Reference [16]

B.8.6.3 Compliance with a Reliability Parameter

Compliance tests are applied to determine whether the reliability performance of an item complies with a specified requirement.

Table B.22—Standard Reference for Compliance Tests

Compliance Test Indicators	Standard Reference
Probability that item performs required function under specified conditions	IEC 61123. Reference [19]
Constant failure rate or intensity	IEC 61124. Reference [20]
Steady state availability	IEC 61070. Reference [21]

B.8.6.4 Comparison of Reliability Performance

Comparison tests are applied to ascertain if the reliability performance of two components is in fact different.

Table B.23—Standard Reference for Comparison Test

Reliability Model Assumption	Standard Reference
Constant failure rate or intensity	IEC 61650. Reference [22]

B.9 Process 9—Performance Tracking and Data Management

B.9.1 Description

RM data are required to:

- inform future safety and risk assessments, reliability, availability and production efficiency analysis;
- monitor current operations and maintenance evaluations and compare with design predictions.

RM data can be collected during various stages in the life of the equipment, during FAT, SIT, installation, commissioning and operation. The majority of current RM data collected for equipment or a system is obtained once the field is operating.

B.9.2 Data Input to Reliability Analysis

RM data is required to inform safety and risk assessments, reliability, availability and production efficiency analysis. It also allows the monitoring of current operations and maintenance evaluations and supports comparisons with design predictions.

Available reliability databases should be interrogated at appropriate times in the design to provide inputs to reliability analysis and reliability assurance. Any available evidence of reliability, including the reliability data, should be investigated and used to inform the reliability analysis carried out at each stage of the design cycle. This directly informs the level of reliability that may be achieved.

For each system, subsystem and component, as appropriate, the expected service conditions should be considered in order that relevant historical data may be identified. This data should be input into the reliability and availability analysis, the results of which demonstrate the achieved reliability in similar conditions and also identify failure modes that have been experienced. The data can also be used to indicate any changes to the design or conditions that should be accounted for in the current project.

B.9.3 Data Collection

Any data capture system should follow and comply with ISO 14224 which defines the minimum requirements of data to be collected, and details the process for ensuring possible exchange/transfer of quality RM data.

OREDA is a joint industry program comprising nine international oil companies. It has the objective of collecting and exchanging RM data to create a larger sample population of required equipment units, (christmas trees, connectors, sensors, etc.) to acquire higher confidence in failure analysis data.

RM data should be collected into databases, spreadsheets or written records to record operating and maintenance information. The following minimum data categories for the equipment and its failure and maintenance events should be captured:

- equipment data;
- identification data, e.g. equipment location, classification, installation data, equipment unit data;
- design data, e.g. manufacturer's data, design characteristics;
- application data, e.g. operation, environment, system, fluid handled;
- failure data;

- identification data, failure record and equipment location;
- failure data for characterizing a failure, e.g. failure date, maintainable items failed, severity class, failure mode, failure cause, method of observation;
- maintenance data;
- identification data, e.g. maintenance record, equipment location, failure record;
- maintenance data, parameters characterizing maintenance, e.g. date of maintenance, maintenance category, maintenance activity, items maintained, maintenance man hours per discipline, active maintenance time, down time.

The data collected should be organized and linked in a computerized database to provide easy access for updates, queries and analysis.

Copyright American Petroleum Institute
Provided by IHS under license with API
No reproduction or networking permitted without license from IHS

B.10 Process 10—Supply Chain Management

B.10.1 Description

It is often found that high-level systems failures with significant consequences originate from the failure of minor components in the system. Systems designer/integrators should understand the significance of the risk potential of all components, including minor components supplied by second and third tier suppliers. Reliability requirements should be allocated down to all components. All suppliers should be capable of managing the various interfaces between the customers and suppliers down the supply chain.

B.10.2 Supplier Capability

The ability to achieve the requirements set within the resource constraints established will depend on the reliability capability maturity of the organization undertaking the relevant task. This includes the timely and adequate completion of RM activities and the delivery, with confidence, of the physical reliability of individual components. The active assessment and selection of vendors and contractors occurs during the FEED and detailed design stages; however, the concept of reliability capability should be considered throughout the project planning stages, especially when delegating task responsibility. Assessments should be based around the KPs identified in this RP and result in a level ranking, such as that defined in Table B.24.

Table B.24—Overview of Reliability Capability Maturity Levels

Maturity Level	Description
1	No understanding of reliability concepts.
2	Prescriptive procedures that are repeatable but do not directly relate to reliability.
3	Understanding of historical achievements in reliability but with limited capability to learn from lessons and improve reliability.
4	Understanding of design for availability and how to correct designs to improve reliability given the observation of failure.
5	Understanding of design for availability and implementation into a proactive continuous improvement program (both managerial and operational).

Reliability capability assessment can either be performed as part of a field development project or as an independent evaluation, depending on the scope of the evaluation.

- Full reliability capability audits should be conducted outside of the field development project. A full capability audit should assess the strengths and weaknesses of an organization's procedures in terms of the KPs recommended in this RP.
- Assessments during supplier/contractor selection should be conducted as a high level review of the potential supplier/contractor with specific regard to the reliability specification. This type of assessment may form part of the customer's specification by requesting evidence/statements of capability.
- Full assessments may be conducted as part of a project to assess, real time, the supplier/contractor reliability capability. This may be viewed as an update or verification of the supplier/contractor capability conducted outside of the project environment.

Reliability capability maturity assessments are applicable to both operators assessing first tier suppliers and first tier suppliers assessing their supply chain. In the case of the latter, the assessment should place emphasis on management of change process through the supply chain. A simplified approach to the assessment procedure is provided below and detailed more comprehensively in Reference [11] and Reference [12]. A more detailed description of the process is outside the scope of this RP.

- Define the elements of the KPs required for the availability strategy (e.g. the activities specified in this RP) and allocate to a KP.
- Describe the performance measures for each of the KP elements.
- Define reliability capability maturity level (see B.10.2) acceptance criteria for each element performance measure. Capability maturity level acceptance criteria should be defined such that achievement of a higher level requires meeting all lower level acceptance criteria.
- Score each of the elements according to the acceptance criteria and determine KP and overall reliability capability maturity levels.
- Compare against required reliability capability maturity levels (e.g. with a spider diagram, see Figure B.4).
- Document recommendations and follow-up actions.

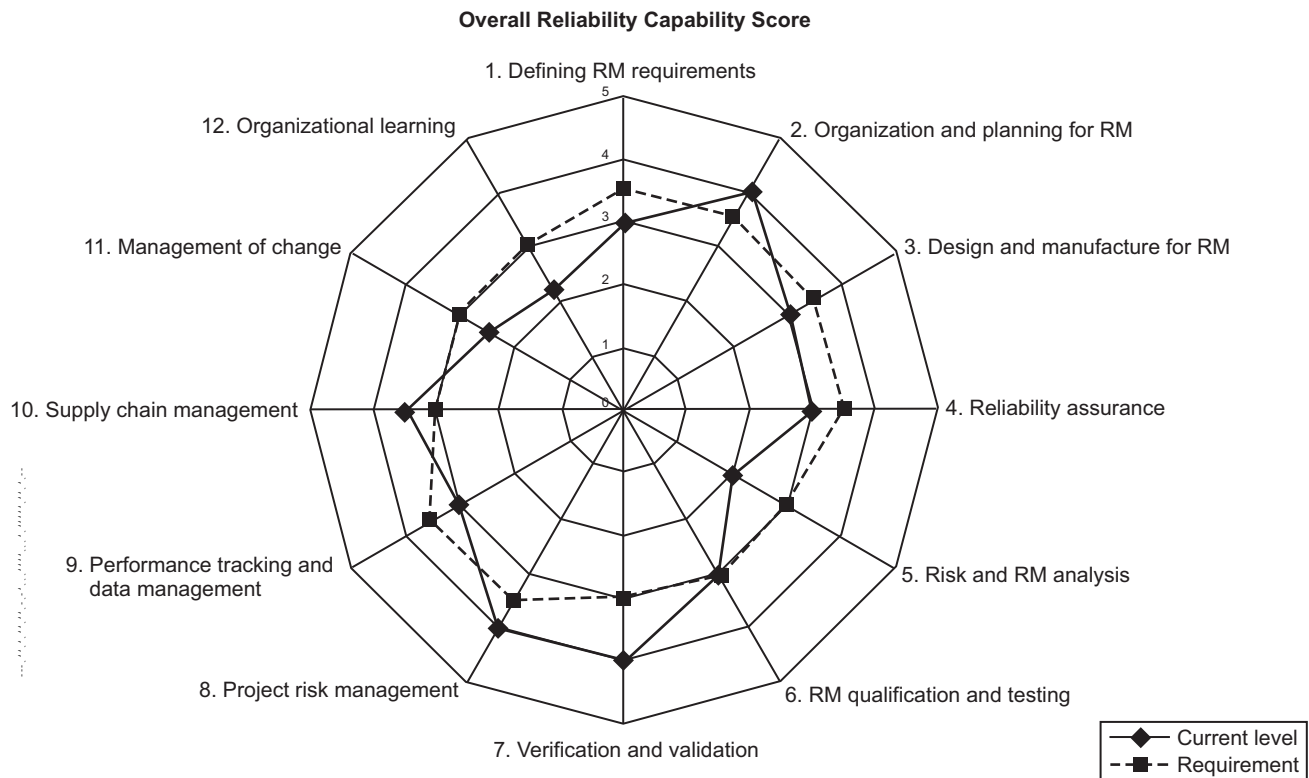


Figure B.4—Example Output from Reliability Capability Maturity Assessment

B.10.3 Contract Strategy

Suppliers are crucial to the success of any field development project and as such have a real opportunity to support the improvement of performance and reliability. Simply seeking the lowest cost supplier may not deliver the greatest value to the project. It is, therefore, recommended that reliability engineering be a part of the contractual agreement between the operator and the contractor. The contracting strategy is an important tool for delivery of value to the project, especially if schemes to incentivize reliability improvement are adopted to provide a win-win solution for operators and contractors alike. Contractual specifications may include:

- quantitative reliability requirements at system, package or component level;
- minimum skills required, for example, in reliability data management or quantitative reliability analysis;
- minimum requirements for reliability activities such as FMECA, RBDA, peer reviews, etc.;
- minimum requirements for internal procedures to address reliability related issues, such as management of change, qualification testing, QA, etc.

B.11 Process 11—Management of Change

B.11.1 Description

Many failures originate from changes made to products or procedures during the life cycle of the product, without due assessment and control. Failures can also be introduced at life cycle stage transitions, due to lack of continuity of ownership of ongoing issues from one stage to the next.

- Companies should have systems in place for change control that include procedures for:
 - monitoring change: to identify the introduction of changes;
 - to recognize when change has to be or has been introduced:
 - from the manufacturer, e.g. design improvements, revisions, upgrades,
 - from the operator, e.g. change in loading, installation, interface or operating requirements;
 - from the subsupplier, e.g. change in material or welding properties, manufacturing tolerances.
- Assessing change: to evaluate any risks introduced to the project as a result of change:
 - to identify the risks and assess the impact these may have on the product/project reliability, either:
 - formally through updating FMECAs, risk reviews, HAZOPS, etc.;
 - informally through design review and peer review processes;
 - it is then necessary to review the categorization of the component, package, or product in the light of the changes that have been made.
- Managing change to control the follow up of necessary actions:
 - to ensure all affected parties are informed of the change and any associated actions are communicated and controlled including:
 - updating of drawings and documentation,
 - revision of analysis (engineering and reliability) and testing,
 - updating the reliability plan and the RAD.
- Monitoring and bench marking changes and follow up actions:
 - to evaluate after the event the impact of the change on:
 - functionality and operability,
 - RM.

The system should be built into the QA system and applied throughout the whole product life cycle to ensure that all changes that affect reliability are formally assessed, managed, documented, communicated and approved through all the project stages.

Of primary importance with microprocessor based control systems is the establishment and adherence of a software change control procedure. The subsea control system equipment supplier should, therefore, in line with the above, demonstrate that an appropriate change control procedure is in place throughout the project life cycle.

B.12 Process 12—Organizational Learning

B.12.1 Description

Each project is a mine of useful knowledge and experience. The collection, review and implementation of lessons learned from previous and current projects is one of the most effective methods of ensuring the same mistakes are not repeated and hence removing historical causes of unreliability. If these lessons are captured, they can be collated and fed back into later projects. Good reliability management should provide resources to ensure that information is fed back to the whole organization involved in design and system integration to allow lessons to be learned and understanding to be gained from experienced failures.

Organizational learning is concerned with the transformation of data and information into intellectual capital of the organization. Intellectual capital takes three main forms:

- 1) human capital: knowledge of individuals in the organization,
- 2) structural capital: knowledge structured in databases and knowledge bases (lessons learned),
- 3) customer capital: knowledge of the company's value to customers.

B.12.2 Learning Competencies

There are four competencies for a learning organization these are:

- absorption of knowledge from the outside (lessons learned capture),
- generation of knowledge within lessons learned capture),
- diffusion and transmission of knowledge within the organization (dissemination),
- exploitation of knowledge in projects.

Table B.25 provides some examples of instruments for learning.

B.12.3 Lessons Learned Capture (Absorption and Generation)

It is recommended that lessons (concerning the successes and failures of the organization) are captured on a formal basis through all projects. These lessons form the input to new projects and should be addressed and considered at every stage of the project as part of the risk and reliability review activities including design reviews. If this is carried out as part of a formal system, then it will be more effective and ensure that it is actually carried out and at the right time.

It is also recommended that every member of the project team be responsible for ensuring that they have each identified and captured all lessons pertinent to their role and area of responsibility within the project.

Lessons relating to the achievement of reliability could include:

- 1) equipment (design, manufacture, installation or operational difficulties);
- 2) procedures (clarity, implementation and approval);
- 3) project management (schedules, budgets, risks).

Lessons can be gathered from a range of sources including; technical experts, project best practices, historical operating and failure data, engineering, test and inspection reports and industry networks (see Table B.25).

Table B.25—Some Instruments for Learning

Absorption	Diffusion	Generation	Exploitation
Professional networks	External coaches/trainers	Information networks	Dialogue
Education	Creation/use of manuals	Job rotation	Self assessment
Conferences	Procedures	Project management	Performance measures
Customer contact	Regulations	Operations feedback	Professional feedback
Competitive analysis	Knowledge information systems	Root cause analyses	Cross discipline teams using know-how to manage projects
Capability assessments	Best practice studies	Final reports	Product and service improvements
Supplier cooperation	Internal knowledge exchange	Simulations	Prototyping
Acquisition	Internal coaching and peer assessments	Quality reviews	Reliable delivery
Contractors R&D		Action learning	

The purpose of the lessons learned review is to facilitate the project risk review process by providing historical evidence of events during the individual project stage.

The lessons learned review is best carried out in conjunction with the project risk review and prior to the commencement of the project risk categorization, so that experience from previous projects can be reviewed. During this task, all relevant data from the previous project should be elicited from appropriate databanks or knowledge management systems. The lessons learned usually cover the whole life of the project from strategic thinking and decision making, through project execution and delivery of the benefits. It is essential that these lessons explicitly address any issues that impact the ability to achieve reliability, from both good and bad practice.

An important tool in Lessons learned capture is RCA of failure (see B.5, Table B.17). This tool facilitates companies in understanding the technical root causes of failure, which in many cases are complex and may involve a variety of factors. It is also possible and good practice to address organizational factors in this process.

B.12.4 Dissemination of Knowledge

For knowledge to be useful, it must be disseminated to those engineers and managers in the project who need this information to make good decisions. Dissemination can be achieved by:

- company experts who take a leading role in providing lessons learned inputs at project reviews and stage gate reviews,
- providing engineers access to lessons learned data/knowledge bases.

These two mechanisms have different implications for the structure of the organization and its information systems. In practice, companies will tend to operate with some combination of the two.

B.12.5 Exploitation of Knowledge in Projects

The tracking, analysis, dissemination and storage of data has most value when the information can be converted into organizational knowledge which adds value to the business and its customers. This may be through improved products and services for delivery of reliability and availability. Exploitation of knowledge will often require additional effort with cross discipline teams to analyze the data, transform it into knowledge and then identify means to exploit the information. This information must then be transmitted to the design team and their managers to ensure that best practice is adopted or best value decisions are made. Often, this may entail R&D to develop prototypes or new products and services. Lessons learned input at a design review early in design e.g. conceptual design or at start of a new project stage, is an important time when such exploitation can be initiated.

B.13 References to Annex B

- [1] US Mil-Std-1629, *Procedures for Performing a Failure Mode Effects and Criticality Analysis*, 1974, 1980 (Rev A), 1984 (Rev A/Notice 2)
- [2] BS 5760 Part 7:1991 ¹, *Guide to Fault Tree Analysis (FTA)*
- [3] BS 5760 Part 9:1994, *Guide to the Block Diagram Technique*
- [4] BS 6079-1:2002, *Guide to Project Management*
- [5] Billinton, R. and Allen, R. (1983), *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, Pitman, London
- [6] Melchers, R. E. (1999), *Structural Reliability Analysis and Prediction*, Second Edition, John Wiley and Sons
- [7] Howard, R. A. (1988), *Decision Analysis: Practice and Promise*, *Management Science*, 34, 679 – 695
- [8] Bedford, T. and Cooke, R. (2001), *Probabilistic Risk Analysis Foundations and Methods*, Cambridge University Press, Cambridge
- [9] Sundararajan, C. (1991), *Reliability Engineering Data, Analysis, Applications, Implementation, and Management*, Van Nostrand Reinhold, New York
- [10] Mobley, K. R. (1999), *Root Cause Failure Analysis*, Elsevier Butterworth-Heinemann
- [11] Strutt, J.E., Sharp, J.V., Terry, E., Miles, R. (2006), "Capability Maturity Models for Offshore Organizational Management," *Environment International*, 32, 1094 – 1105
- [12] Sharp, J.V., Strutt, J.E., Terry, E. (2002), *Measurement of Organisational Maturity in Designing Safe Offshore Installations*, Proceedings of OMAE
- [13] IEC 60605-6:1997 ², *Equipment Reliability Testing. Tests for the Validity of the Constant Failure Rate or Constant Failure Intensity Assumptions*
- [14] IEC 61649:1997, *Procedures For Goodness-of-Fit Tests, Confidence Intervals and Lower Confidence Limits for Weibull Distributed Data*
- [15] IEC 61710:2000, *Power law model. Goodness-of-Fit Tests and Estimation Methods*

¹ BSI British Standards, 389 Chiswick High Road, London W4 4AL, United Kingdom, www.bsi-global.com.

² International Electrotechnical Commission, 3, rue de Varembé, P.O. Box 131, CH-1211, Geneva 20, Switzerland, www.iec.ch.

- [16] IEC 61164:1995, *Reliability of Systems, Equipment and Components. Reliability Growth. Statistical Test and Estimation Methods*
- [17] IEC 62198:2001, *Project Risk Management. Application Guidelines*
- [18] IEC 60605-4:2001, *Equipment Reliability Testing. Statistical Procedures for Exponential Distribution. Point Estimates, Confidence Intervals, Prediction Intervals and Tolerance Intervals*
- [19] IEC 61123:1991, *Reliability of Systems, Equipment and Components. Guide to Reliability Testing. Compliance Test Plans for Success Ratio*
- [20] IEC 61124:1997, *Reliability Testing, Compliance Tests for Constant Failure Rate and Constant Failure Intensity*
- [21] IEC 61070:1991, *Reliability of Systems, Equipment and Components, Guide to Reliability Testing. Compliance Test Procedures for Steady-state Availability*
- [22] IEC 61650:1997, *Reliability Data Analysis Techniques, Procedures for Comparison of Two Constant Failure Rates and Two Constant Failure (Event) Intensities*
- [23] ISO 14224 ³, *Petroleum, petrochemical and natural gas industries—Collection and exchange of reliability and maintenance data for equipment*

³ International Organization for Standardization, 1, ch. de la Voie-Creuse, Case postale 56, CH-1211, Geneva 20, Switzerland, www.iso.org.

Annex C **(informative)**

Reliability Data Management

This annex provides specific guidance on the collection and management of reliability and performance data to best support reliability implementation.

C.1 Objectives

Achieving very high reliability performance requires knowledge of at least three areas which should be supported by data collection in order to have acceptable scientific evidence on which to base any future (design) engineering, process and organizational improvement action:

- What current performance is being achieved?
- What should/might be changed to improve that performance?
- What is the economic incentive for doing so?

The objective of the reliability “data collection” activities is to provide this qualified, quantitative evidence of product design, installation and operational performance and field usage for use in future system development (performance improvement) and to provide early warning of reliability issues before the consequence of failure become unacceptable.

Definition of Success

A data collection process for this RP which captures sufficient, appropriate and detailed data and information to:

- establish a product history (build, application and use with time sequence);
- identify, predict and prevent repeat failures from the same root cause;
- illuminate lessons learned to both prevent replication of error and enable copy and repetition of success.

C.2 Assumptions

The “buyer” will ensure that all vendors in the supply chain are at least ISO 9001:2000 [2] certified or supply their manufactured goods through a party who holds such certification.

This will provide at least minimum assurance that adequate records are created and maintained with respect to the manufacturing processes to allow detailed RCA if it should prove necessary in a future investigation.

As new technology is introduced, it is likely that some of those manufacturing processes will be proprietary and whilst we should expect the manufacturer to have appropriate records of the specific processes related to the particular product by serial number this information would remain confidential.

C.3 Overview

A key driver of reliability performance improvement as described elsewhere in this RP is better understanding of failure mechanisms and root causes. It is not easy to define a data collection process which provides the level of detail required to do thorough failure investigations leading to an understanding of root causes and at the same time has the limited complexity and open access required of a shared database to be used by many.

Equipment failures can be the result of a combination of factors such as small defects, insignificant damage, less than perfect installation and inability to detect small defects during testing. Equipment failures can also be the result of design errors or inadequate design processes—organization and processes. As recognized in ISO 14224 [3], it is essential to be able to capture and create a good lesson learned database.

It is also important to have a generic equipment hierarchy or taxonomy which fits the real world. This should be sufficiently flexible to permit the inclusion of different field architectures and concepts. ISO 14224 recommends the setting of appropriate system boundaries to avoid duplication of data and, then provides a suitable taxonomy on which to base the data collection process. For the purpose of this RP, the boundaries described in API 17A [1] have been adopted as noted and illustrated above.

The capture and collection of maintenance data to reflect downtime (consequences) is addressed in some detail in ISO 14224 together with the necessary data structure needed to do so. Such information is only valuable if it can be associated with geographical location, water depth, resource contacting strategy, management of change, etc. so that the sensitivity of related specific failure events, mechanisms and root causes to these parameters can be revealed.

C.4 Scope

The collection process is illustrated visually in ISO 14224 by the diagram shown below.

The scope for subsea reliability data collection encompasses data relating to all equipment installed subsea within the boundaries described in API 17A for the purpose noted above, namely “to establish product performance (usage) history for further evaluation in engineering analysis for system improvements, for new system developments and avoidance of intolerable failures.”

Data to be collected can be categorized under four main headings:

- equipment data (design);
- application data (usage);
- in-service data:
 - failure data;
 - maintenance data (preventive and corrective), including well intervention and workover data.

C.5 Strategy

The strategy for data collection can be summarized in Figure C.1 and as follows.

- 1) Data should be collected by the originator as close to the time and point of its origin as possible. This helps to reduce ambiguity in the responsibilities for data collection and ensures the highest possible level of data quality.
- 2) The responsibility for data collection, therefore, changes as a project moves through the life cycle.
 - a) Equipment suppliers/vendors and manufacturers are responsible for collection of equipment specific data, i.e. the design and manufacturing data.
 - b) Installation data are to be captured by the installer where he/she is the equipment supplier. In case of a third party installer, the installation data are to be captured by the operator.
 - c) Operators are responsible for collection of the application aspects of the equipment, i.e. usage, environmental aspects, process conditions, locations, etc.

- d) There is necessarily joint responsibility for in-service data such as maintenance or failure data (operator provides data relating to time place and circumstances, manufacturer provides RCA data after investigation).
- 3) The one who is responsible for collecting the data is also responsible for storing the data in a retrievable format. Either party may provide fields in their data system for the other party's data to enable and facilitate the exchange of data.

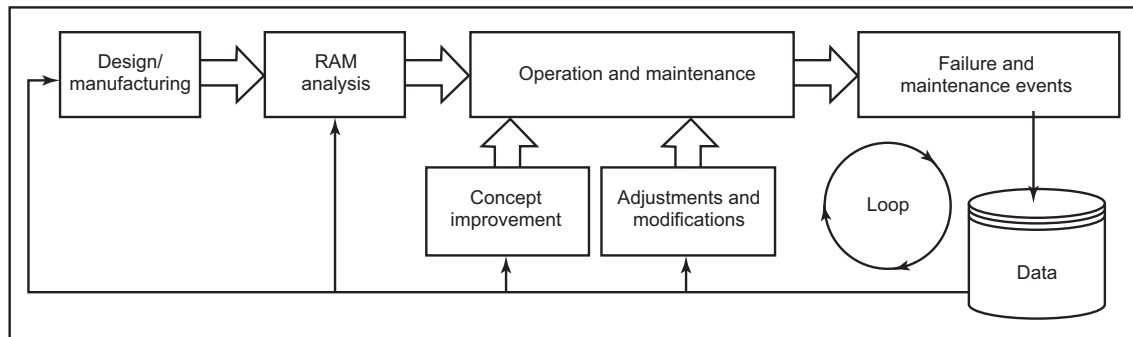


Figure C.1—Data Collection and Usage Strategy

It is essential to remember that the purpose of data collection is to provide performance evidence to support or deny reliability claims and provide a scientific justification for future activities. If the data lacks adequate detail and accuracy to serve this purpose the effort spent collecting it has been wasted. It should be possible to identify root cause where failures are concerned and actual operating regimes where frequency information is sought.

C.6 Reliability Data

Equipment Suppliers/vendors

Equipment suppliers should capture any equipment specific data, where possible including “lessons learned” during the detailed design and testing stage, providing subsequent valuable information on design limitations and allowable operating envelope for the operator and help direct improvement effort for future systems.

Typical information collected will include:

- serial numbers;
- material specifications;
- manufacturing processes (welding procedures, treatment processes, etc.);
- applicable design codes;
- equipment application (pressure, temperature rating, etc.);
- equipment description (part numbers);
- FAT/SIT results;
- qualification tests results;
- lessons learned.

Operators

Operators should capture the application, operating environment and usage of the equipment. In addition operational inconsistencies, equipment failures and maintenance interventions performed on the subsea equipment should be recorded.

Typical data to be collected include:

- life of field operating conditions, flow rate, pressures, sand production, water production, gas-to-oil ratio (GOR), etc.;
- geographical location, including water depth, and relevant metocean data;
- equipment in-service information (storage of equipment, out of service, batch installation, etc.);
- failure information, including specific failure description and failure root cause and causal factors;
- maintenance data, if equipment is taken out of service, replaced or adjusted;
- management of change (equipment application changed, changer of service).

C.7 Measurement of Success

How do we obtain data about success (confirming availability goals are achieved) apart from an absence of failure data?

There are at least two approaches to consider:

- normal signature—continuous monitoring of normal operating parameters,
- condition inspection of equipment removed from service.

Normal Signature

All systems have a normal signature—the operating parameters once the system has bedded down—which should be monitored. Variations in these parameters outside the “normal” range will be a precursor to an anomalous event and may predict incipient failure if other explanations are not forthcoming. Even if there is an explanation, that event may itself be a trigger for a future failure and should be analyzed carefully.

Removed Equipment Inspection

Equipment removed for any reason—not just failure—should be inspected to determine if its condition is as expected. Are the wear rates, corrosion levels, etc. as expected, better or worse? This data can be used to modify life expectancy under similar operating regimes and in similar environments.

Equipment Log-book

In aviation and automotive applications, log-books are used to create a permanent record of maintenance and change activities relating to the equipment, e.g. an aircraft and its subsystems. This same technique could be adopted for subsea systems. In cases where maintenance is limited to inspection, say by ROV, these could be logged together with the results of function checks against a check-list. These “inspections” might be based on calendar time, operating time or production throughput or other pertinent parameters (number of start-ups or shut-ins, etc.) determined by the designers during the system development stage of the project.

Summary log-book information can be collected at each entry trigger as part of the evidence of success and/or progressive degradation not categorized as failure (e.g. reduced speed of valve operation).

NOTE Equipment manufacturers, suppliers and or contractors are not bound by this document to provide or acquire specific reliability data.

C.8 References to Annex C

- [1] API Recommended Practice 17A, *Design and Operation of Subsea Production Systems—General Requirements and Recommendations*
- [2] ISO 9001:2000 ⁴, *Quality Management Systems—Requirements*
- [3] ISO 14224:2006, *Petroleum and natural gas industries—Collection and exchange of reliability and maintenance data for equipment*
- [4] Farit M. Akhmedjanov (2001), *Reliability Databases: State-of-the-Art and Perspectives*, Riso National Laboratory, Pitney Bowes Management Services, ISBN 87-550-2809-8

⁴ International Organization for Standardization, 1, ch. de la Voie-Creuse, Case postale 56, CH-1211, Geneva 20, Switzerland, www.iso.org.

Annex D (informative)

Application of Test Statistics

This annex provides example methods for estimating the failure rate of equipment from performance verification test data. (It is not appropriate to use this method in reverse to determine the level of testing needed to achieve a failure rate performance requirement.)

D.1 Application of Test Statistics of Continuous Operation Components

This example demonstrates how the reliability of a device can be estimated from tests conducted in conditions equivalent to those expected in operation from a sample number of components. For further information, including reliability growth methods, refer to Reference [1].

Recorded times to failure are generally subjected to a number of statistical tests with the objective of:

- validating the failure pattern [e.g. a constant hazard rate (CHR) (see note)],
- estimating the reliability parameters (e.g. the mean time to failure).

NOTE The minimum number of tests to failure to indicate that the pattern has a CHR is 4, but ideally, for greater confidence, a larger population should be used.

Table D.1 provides a set of sample data for the purposes of this example. It is assumed that 20 items were tested under the expected operating conditions and the test was concluded when the final item failed. All failures are assumed relevant.

Table D.1—Example of Sorted Failure Data

Failure Number	Time to Item Failure (Yr)	Failure Number	Time to Item Failure	Failure Number	Time to Item Failure
1	0.055693	8	1.43274	15	2.38448
2	0.12863	9	1.63482	16	3.14187
3	0.30204	10	1.64809	17	3.25363
4	0.32808	11	1.77079	18	3.6551
5	0.53285	12	1.8526	19	4.29491
6	0.80301	13	1.85436	20	7.8356
7	0.98767	14	1.89738		

D.1.1 Test for Validating Failure Pattern

This example provides a numerical procedure to test the assumption that a set of recorded failures exhibits a constant failure rate.

For $i = 1$ to r , calculate the accumulated time, T_i , to the i th failure as:

$$T_i = (n - i)t_i + \sum_{k=1}^r t_k \quad (1)$$

Calculate the total accumulated test time, T^* , as:

$$T^* = (n-r)t_r + \sum_{k=1}^r t_k \quad (2)$$

where

n is the number of samples in the test;

t_i is the time of the i th failure;

t_r is the time of the last (r th) failure;

r is the number of failed items in the test sample.

NOTE where $n = r$; $T_r = T$.

Table D.2 gives T_i values for this example.

Table D.2—Example T_i Values

Failure Number	Accumulated Test Time, T_i	Failure Number	Accumulated Test Time, T_i	Failure Number	Accumulated Test Time, T_i
1	1.11386	8	21.763593	15	29.535633
2	2.499663	9	24.188553	16	33.322583
3	5.621043	10	24.334523	17	33.769623
4	6.063723	11	25.561523	18	34.974033
5	9.340043	12	26.297813	19	36.253653
6	13.392443	13	26.311893	20	39.794343
7	15.977683	14	26.613033		

For a test set between 10 and 40 items, calculate the chi-squared statistic, X^2 , for set as:

$$X^2 = 2 \sum_{i=1}^d \ln\left(\frac{T^*}{T_i}\right) \quad (3)$$

where

d is the degree of freedom. If the test is concluded when an item fails then $d = r - 1$, otherwise $d = r$.

In the example provided, the chi-squared statistic is $X^2 = 35.52$

Compare the chi-squared statistic with the theoretical values of chi-squared, $X^2(\nu)$, where $\nu = 2d$.

Perform a two-sided test, for a 10 % significance level, as follows:

If $X^2 < X^2_{0.05}(\nu)$ then reject the assumption of a constant failure rate as the failure rate is likely to be increasing.

If $X^2 > X^2_{0.95}(\nu)$ then reject the assumption of a constant failure rate as the failure rate is likely to be decreasing.

In this example, for $\nu = 38$, $X^2_{0.05}(38) = 24.91$ and $X^2_{0.95}(38) = 53.36$.

NOTE These values are acquired from a chi-squared distribution table.

In this example, $X_{0.95}^2(38) > 35.52 > X_{0.05}^2(38)$, therefore, the assumption that the data are observing a constant failure rate is valid.

Should the data fail this test, then the data should be tested to validate the assumption that the failure rate is either increasing or decreasing.

D.1.2 Estimating the Failure Parameter

Having determined that the item failure pattern follows a CHR, the failure rate can be estimated as follows.

A point estimate of the failure rate, $\hat{\lambda}$, is given by:

$$\hat{\lambda} = \frac{r}{T^*} \quad (4)$$

To calculate the upper and lower bound confidence limit, first specify a confidence interval, $1 - \alpha$. The lower limit of the failure rate, λ_{L2} , is calculated as:

$$\lambda_{L2} = \frac{X_{\alpha/2}^2(2r)}{2T^*} \quad (5)$$

The upper limit of the failure rate, λ_{U2} , is calculated as:

$$\lambda_{U2} = \frac{X_{1-\alpha/2}^2(2r)}{2T^*} \quad (6)$$

With the example data provided, the point estimate is calculated as:

$$\hat{\lambda} = \frac{20}{39.79} \approx 0.5 \quad (7)$$

This corresponds to a mean time to failure of 2 years. Assuming that 90 % confidence is required between the upper and lower bound estimates (i.e. = 10 %), the lower limit of the failure is calculated as:

$$\lambda_{L2} = \frac{X_{\alpha/2}^2(2r)}{2T^*} = \frac{X_{0.05}^2(20)}{79.58} = \frac{26.51}{79.58} = 0.33 \quad (8)$$

Which corresponds to a mean time to failure of 3 years; the upper limit is calculated as:

$$\lambda_{U2} = \frac{X_{1-\alpha/2}^2(2r)}{2T^*} = \frac{X_{0.95}^2(20)}{79.58} = \frac{55.76}{79.58} = 0.69 \quad (9)$$

This corresponds to a mean time to failure of 1.45 years.

D.2 Application of Test Statistics for Non-continuous Operation

Performance verification of equipment is often drawn from API 6A and API 17D cycle test requirements, intended to validate non-continuous operating cycle life for an assumed design (or operating life). Since these concepts are often

limited, and statistical averages may not be readily obtained, cycle tests are used to demonstrate performance verification for the assumed design life

Ideally, MTBF values are based on observed data as their basis (demonstrated value) or are based upon reported failures (reported value). However, demonstrated or reported values may be difficult to obtain because of the small sample size or the uncertainty associated with true operating conditions. Therefore, this calculation method may be used to estimate MTBF until proper field data become available. The chi-square distribution (χ^2 distribution) is used to estimate the uncertainty of the reliability estimate of API 6A/API 17D performance verification tests, assuming that bench-test failures occur randomly (as opposed to infantile or wear-out failures). However, if random failure distribution assumption is invalid, the results from Equation (10) could be misleading.

Calculating the lower confidence bound on an MTBF is given by the following equation:

$$\text{lower limit}_{\text{cycles}} = \frac{2T_{(\text{cycles})}}{\chi^2_{(2r+2, \alpha)}} \quad (10)$$

where

- T is the total number of cycles a component sees during a test;
- r is the number of failures occurring during the test interval T ;
- α is the interval such that $(1 - \alpha)$ is the lower confidence factor of the MTBF;
(e.g. 50 % confidence $\rightarrow \alpha = 0.5$; 30 % confidence $\rightarrow \alpha = 0.7$);

lower limit is the MTBF, where MTBF is defined as the point in time (or cycles) where reliability has decreased to 67 %.

NOTE 1 In mathematical terms for χ^2 , $(2r + 2)$ is referred to as the degree of freedom variable, and α is referred to as the non-centrality function.

NOTE 2 Where replicate tests are practicable, it is recommended that these are included to check that the distribution conforms to CHR or to improve confidence in the lower bound MTBF estimate. A minimum of four tests would normally be necessary to check conformance to CHR.

Once the lower limit is established for a given number of failures and confidence factor, the component's reliability can be estimated using the following equation:

$$RFT_{(\text{cycles})} = e^{-(\text{field cycles}/\text{lower limit})} \quad (11)$$

where

- RFT is the reliability of the component, estimated from tests, for a given number of field cycles.

NOTE 3 The term RFT has been introduced here to emphasize that the reliability is estimated from test(s) rather than historical field failure performance. The value of reliability obtained from tests has a different interpretation from that derived from historical failure data and is sensitive to the test conditions. Test conditions should be made explicit.

D.2.1 Confidence Factor

The confidence factor is a statistical variable that describes the probability of certainty in the “lower limit” value. Lowering the confidence factor increases (more optimistic) the value of the lower limit (MTBF). A very high confidence factor is interpreted as a very conservative estimate for the lower limit.

Confidence Factor $P_x (1 - \alpha)$	α	$\chi^2 (2r + 2, \alpha)$		
		$r = 0$	$r = 1$	$r = 2$
P_{10} (10 %)	0.9	0.211	1.064	2.204
P_{20} (20 %)	0.8	0.446	1.649	3.070
P_{25} (25 %)	0.75	0.575	1.923	3.455
P_{30} (30 %)	0.7	0.713	2.195	3.828
P_{40} (40 %)	0.6	1.022	2.752	4.570
P_{50} (50 %)	0.5	1.386	3.357	5.348
P_{60} (60 %)	0.4	1.833	4.045	6.211
P_{70} (70 %)	0.3	2.408	4.878	7.231
P_{75} (75 %)	0.25	2.773	5.385	7.841
P_{80} (80 %)	0.2	3.219	5.989	8.558
P_{90} (90 %)	0.1	4.605	7.779	10.645
P_{99} (99 %)	0.01	9.210	13.277	16.812

P_{50} and $r = 0$ should be used to correlate the χ^2 function and its estimated MTBF when predicting reliability for performance verification tests found in API 17D or API 6A.

D.2.2 Examples for Calculating MTBF

EXAMPLE 1

Consider a choke stepping actuator's cycle testing completing a 1,000,000 cycle test with no failures ($r = 0$). What is its reliability, for a 50 % confidence, as a function of field cycles for the field unit?

Calculating the lower confidence bound on an MTBF is given by the following equation:

$$\text{lower limit} = \frac{2T}{\chi^2_{(2r+2, \alpha)}} = \frac{2(1,000,000)}{\chi^2_{(2, 0.5)}} = \frac{2,000,000}{1,386} = 1,443,000 \text{ cycles} \quad (12)$$

Interpretation: “There is 50 % confidence that the mean cycles-to-failure of the actuator is at least 1,443,000.”

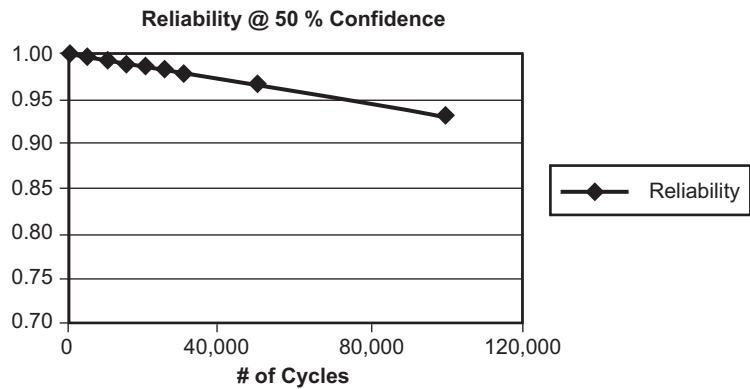
$$\text{MTBF}_{(\text{cycles})} = 1,443,000 \quad (13)$$

Applying the exponential reliability equation:

$$R_{(\text{cycles})} = e^{-(\text{field cycles} / 1,443,000)} \quad (14)$$

The results at 50 % confidence are as follows.

# of Field Cycles	Reliability
0	1.000
5,000	0.997
10,000	0.993
15,000	0.990
20,000	0.986
25,000	0.983
30,000	0.979
50,000	0.966
100,000	0.933



Assuming that the actuator performs 500 cycles per year:

$$MTBF_{(years)} = 1,443,000/500 = 2,886 \text{ years} \quad (15)$$

EXAMPLE 2

Consider a valve cycle testing to failure is 723 cycles before it malfunctions ($r = 1$). What is its MTBF, for a 50 % confidence?

Calculating the Lower confidence bound on an MTBF is given by the following equation:

$$\text{lower limit} = \frac{2T}{X^2_{(2r+2, \alpha)}} = \frac{2(723)}{X^2_{(4, 0.5)}} = \frac{1,446}{3,357} = 431 \text{ cycles} \quad (16)$$

Interpretation: "There is 50 % confidence that the mean cycles-to-failure of the valve is at least 431."

$$MTBF_{(cycles)} = 431 \quad (17)$$

Assuming that the valve performs 12 cycles per year:

$$MTBF_{(years)} = 431/12 = 35.9 \text{ years} \quad (18)$$

The MTBF values obtained from this method should only be considered a starting point value and should be followed up by a risk assessment process to determine if additional scope of qualification testing is needed to meet specific reliability requirements such as described in B.8, or as detailed in API 17Q.

D.3 References for Annex D

- [1] IEC 61164:1995⁵, *Reliability growth—Statistical Test and Estimation Methods*
- [2] O'Connor, P.D.T. (2002), *Practical Reliability Engineering*, Fourth Edition, Wiley

⁵ International Electrotechnical Commission, 3, rue de Varembe, P.O. Box 131, CH-1211, Geneva 20, Switzerland, www.iec.ch.

Copyright American Petroleum Institute
Provided by IHS under license with API
No reproduction or networking permitted without license from IHS



2009

Publications

Order Form

Effective January 1, 2009.

API Members receive a 30% discount where applicable.

The member discount does not apply to purchases made for the purpose of resale or for incorporation into commercial products, training courses, workshops, or other commercial enterprises.

Available through IHS:

Phone Orders: **1-800-854-7179** (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: **303-397-2740**
Online Orders: **global.ihs.com**

Date: _____

☐ **API Member** (Check if Yes)

Invoice To (☐ Check here if same as "Ship To")

Name: _____

Title: _____

Company: _____

Department: _____

Address: _____

City: _____ State/Province: _____

Zip/Postal Code: _____ Country: _____

Telephone: _____

Fax: _____

Email: _____

Ship To (UPS will not deliver to a P.O. Box)

Name: _____

Title: _____

Company: _____

Department: _____

Address: _____

City: _____ State/Province: _____

Zip/Postal Code: _____ Country: _____

Telephone: _____

Fax: _____

Email: _____

Quantity	Title	SO ★	Unit Price	Total
	Spec Q1/ISO TS 29001, Specification for Quality Programs for the Petroleum and Natural Gas Industry		\$102.00	

☐ Payment Enclosed ☐ P.O. No. (Enclose Copy) _____

☐ Charge My IHS Account No. _____

☐ VISA ☐ MasterCard ☐ American Express

☐ Diners Club ☐ Discover

Credit Card No.: _____

Print Name (As It Appears on Card): _____

Expiration Date: _____

Signature: _____

Subtotal

Applicable Sales Tax (see below)

Rush Shipping Fee (see below)

Shipping and Handling (see below)

Total (in U.S. Dollars)

★ To be placed on Standing Order for future editions of this publication, place a check mark in the SO column and sign here:

Pricing and availability subject to change without notice.

Mail Orders – Payment by check or money order in U.S. dollars is required except for established accounts. State and local taxes, \$10 processing fee, and 5% shipping must be added. Send mail orders to: **API Publications, IHS, 15 Inverness Way East, c/o Retail Sales, Englewood, CO 80112-5776, USA.**

Purchase Orders – Purchase orders are accepted from established accounts. Invoice will include actual freight cost, a \$10 processing fee, plus state and local taxes.

Telephone Orders – If ordering by telephone, a \$10 processing fee and actual freight costs will be added to the order.

Sales Tax – All U.S. purchases must include applicable state and local sales tax. Customers claiming tax-exempt status must provide IHS with a copy of their exemption certificate.

Shipping (U.S. Orders) – Orders shipped within the U.S. are sent via traceable means. Most orders are shipped the same day. Subscription updates are sent by First-Class Mail. Other options, including next-day service, air service, and fax transmission are available at additional cost. Call 1-800-854-7179 for more information.

Shipping (International Orders) – Standard international shipping is by air express courier service. Subscription updates are sent by World Mail. Normal delivery is 3-4 days from shipping date.

Rush Shipping Fee – Next Day Delivery orders charge is \$20 in addition to the carrier charges. Next Day Delivery orders must be placed by 2:00 p.m. MST to ensure overnight delivery.

Returns – All returns must be pre-approved by calling the IHS Customer Service Department at 1-800-624-3974 for information and assistance. There may be a 15% restocking fee. Special order items, electronic documents, and age-dated materials are non-returnable.

THERE'S MORE WHERE THIS CAME FROM.

API provides additional resources and programs to the oil and natural gas industry which are based on API Standards. For more information, contact:

API MONOGRAM® LICENSING PROGRAM

Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API QUALITY REGISTRAR (APIQR®)

- > ISO 9001 Registration
- > ISO/TS 29001 Registration
- > ISO 14001 Registration
- > API Spec Q1® Registration

Phone: 202-962-4791
Fax: 202-682-8070
Email: certification@api.org

API PERFORATOR DESIGN REGISTRATION PROGRAM

Phone: 202-682-8490
Fax: 202-682-8070
Email: perfdesign@api.org

API TRAINING PROVIDER CERTIFICATION PROGRAM (API TPCP™)

Phone: 202-682-8490
Fax: 202-682-8070
Email: tpcp@api.org

API INDIVIDUAL CERTIFICATION PROGRAMS (ICP®)

Phone: 202-682-8064
Fax: 202-682-8348
Email: icp@api.org

API ENGINE OIL LICENSING AND CERTIFICATION SYSTEM (EOLCS)

Phone: 202-682-8516
Fax: 202-962-4739
Email: eolcs@api.org

API PETROTEAM (TRAINING, EDUCATION AND MEETINGS)

Phone: 202-682-8195
Fax: 202-682-8222
Email: petroteam@api.org

API UNIVERSITY™

Phone: 202-682-8195
Fax: 202-682-8222
Email: training@api.org

Check out the API Publications, Programs, and Services Catalog online at www.api.org.



Copyright 2008 – API, all rights reserved. API, API monogram, APIQR, API Spec Q1, API TPCP, ICP, API University and the API logo are either trademarks or registered trademarks of API in the United States and/or other countries.

11/11/2011 11:11:11 AM



1220 L Street, NW
Washington, DC 20005-4070
USA

202.682.8000

Additional copies are available through IHS
Phone Orders: 1-800-854-7179 (Toll-free in the U.S. and Canada)
303-397-7956 (Local and International)
Fax Orders: 303-397-2740
Online Orders: global.ihs.com

Information about API Publications, Programs and Services
is available on the web at www.api.org

Product No. G17N01