Recommended Practice on Subsea Production System Reliability, Technical Risk, and Integrity Management

API RECOMMENDED PRACTICE 17N
SECOND EDITION, JUNE 2017

AMERICAN PETROLEUM INSTITUTE

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.

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.

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.

The verbal forms used to express the provisions in this document are as follows.

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

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

May: As used in a standard, “may” denotes a course of action permissible within the limits of a standard.

Can: As used in a standard, “can” denotes a statement of possibility or capability.

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, NW, Washington, DC 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, NW, Washington, DC 20005.

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

Contents

Contents

Contents

Introduction

Reliability and integrity can have major environmental, safety, and financial impacts for all organizations involved in designing, manufacturing, installing, and operating subsea equipment. The complexity of technical and organizational challenges in subsea projects and operations requires continual attention to detail to achieve high reliability and integrity performance.

Equipment reliability is important both to system integrity and to production. For example, poor seal reliability in a flow line connector may result in loss of containment with the potential for environmental damage. Valves that fail to close on command may prevent isolation and compromise safety. Valves that fail to open on command may compromise production.

Budget and schedule constraints can lead to limited information and time for making decisions. This can introduce varying levels of uncertainty that have the potential to affect equipment reliability, integrity, and associated operational risks. In particular, any potential failures that lead to loss of containment or loss of production should be thoroughly investigated and actions taken to manage the risks that such events generate.

This recommended practice (RP) provides a structured approach that organizations can adopt to manage technical uncertainty throughout the life cycle of a subsea system. This may range from the management of general project risk through to the identification and mitigation of potential equipment failure modes, affecting integrity or production.

Most organizations will find much that is familiar and recognized as good practice. Some sections of the annexes may only be of interest to the reliability and integrity specialist. The basic approach, however, is simple and consistent and when applied correctly has the potential to greatly reduce the financial, safety, and reputational risks, arising from potential failures, throughout the life cycle of subsea systems.

Although this RP is focused on subsea production equipment, the guidance is generic and may be easily adapted to address the design of subsea hardware used for drilling operations including the subsea blowout preventer and lower marine riser package.

Recommended Practice on Subsea Production System Reliability, Technical Risk, and Integrity Management

1 Scope

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

— standard and nonstandard equipment (within the scope of API 17A);

— new field developments, further development of existing fields and field upgrades;

— all life cycle phases from feasibility through design, manufacture, and operation to decommissioning.

NOTE API 18LCM [1] gives additional guidance on general requirements for life cycle management of equipment.

This RP is **not** intended to replace individual company processes, procedures, document nomenclature, or numbering; it is a guide. For example, this RP does not prescribe the use of any specific equipment or process. It does not recommend any actions, beyond good engineering practice. However, this RP may be used to enhance existing processes, if deemed appropriate.

2 Normative References

The following normative documents contain provisions that, through reference in this text, constitute provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. For undated references, the latest edition of the normative document applies.

API Recommended Practice 17A, *Design and Operation of Subsea Production Systems—General Requirements and Recommendations*

API Recommended Practice 17Q, *Technology Qualification for Subsea Equipment*, Second Edition

NOTE API 17Q, Second Edition is planned for publication in 2017. Annexes E and F are included in this document to provide interim guidance and will be removed once API 17Q, Second Edition is published. For all references in the text to API 17Q, the reader should refer to these annexes until API 17Q is published.

API Recommended Practice 75, *Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities*

API Recommended Practice 580, *Risk-Based Inspection*

BS [1] IEC [2] 62198:2001, *Project risk management—Application guidelines*

DNV-RP-A203 [3], *Technology Qualification*, July 2013

IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems*

---

[1] British Standards Institution, 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.

[3] DNV GL, Veritasveien 1, 1363 Hovik, Norway, www.dnvgl.com.

ISO 14224 [4], *Petroleum, petrochemical and natural gas industries—Collection and exchange of reliability and maintenance data for equipment*

ISO 20815, *Petroleum, petrochemical and natural gas industries—Production assurance and reliability management*

3 Terms, Definitions, Acronyms, and Abbreviations

3.1 Terms and Definitions

For the purposes of this standard, the following terms and definitions apply.

3.1.1
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 over a given time interval, assuming that the required external resources are provided.

NOTE The term "ability" is often interpreted as probability.

3.1.2
availability requirements
Appropriate combination of reliability and/or maintainability performance characteristics that need to be achieved to meet project requirements.

3.1.3
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 one 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.

3.1.4
confidence interval
A confidence interval is a term used in inferential statistics that measures the probability that a population parameter will fall between two set values.

NOTE The confidence interval can take any probability values, with the most common being 90 % or 95 %.

3.1.5
configuration management
CM
A management process that establishes and maintains consistency of a product's attributes with the requirements and product configuration information (i.e. product design, realization, verification, operation, and support) throughout the product's life cycle.

3.1.6
critical systems
Critical systems are those for which a failure will lead to major accidents (i.e. safety critical systems), loss of containment (i.e. environmental critical systems), or significant loss of production (i.e. production critical systems).

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

3.1.7
downtime
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).

3.1.8
environment
The internal, external, and operational conditions to which equipment are exposed.

NOTE This includes physical, chemical, biological, and usage conditions (i.e. seawater environment, water depth, seabed conditions, reservoir conditions, pressure, temperature, etc.).

3.1.9
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 a fault, which is a state.

3.1.10
failure data
Information related to the occurrence of a failure event.

3.1.11
failure impact (effect)
Consequence of a failure on a system, on an equipment function, on the economy, on human safety, or on the environment.

3.1.12
failure mechanism
A process (physical, chemical, human, or other) that leads to a failure.

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

3.1.13
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).

3.1.14
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.

3.1.15
frequency
(a) The number of occurrences of a specified event or class of events per unit time, cycles, or other measures.

(b) The ratio of the number of times an event occurs in a series of trials of a chance experiment relative to the number of trials of the experiment performed.

NOTE 1 Definition (a) is assumed wherever the term frequency is used, unless otherwise stated.

NOTE 2 In this RP, definition (b) is equivalent to the definition of probability.

3.1.16
function
The intended purpose of an item to perform a specific task or capability.

3.1.17
hazard
A situation with the potential for harm or loss of system or damage to the environment, the term includes danger to persons arising within a short timescale (e.g. fire and explosion) and also those that have a long-term effect on a person's health (e.g. release of a toxic substance).

3.1.18
human error
That which involves deviation from an intended action due to slips, lapses, or mistakes.

NOTE Human error can also be the result of processes with inadequate procedural controls.

3.1.19
human factors evaluation
Use of various methods (e.g. function and task analysis, human-system interface reviews, training reviews, procedure reviews, incident investigations) in order to identify sources and potential effects of human error.

3.1.20
installation hardware
The system or equipment used to install subsea production hardware.

3.1.21
integrity
The ability of a system of components to perform its required function while preventing or mitigating incidents that could pose a significant threat to life, health, and the environment over its operating life.

NOTE The term "ability" is often interpreted as probability.

3.1.22
integrity management
The systematic implementation of the activities necessary to ensure that critical systems are properly designed and installed in accordance with specifications, and remain fit for purpose until they are decommissioned.

3.1.23
maintainability
The 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.

NOTE The term "ability" is often interpreted as probability.

3.1.24
maintenance record
Set of data that contains all failure, fault, and maintenance information relating to an item.

3.1.25
maintenance-free operating period
MFOP
The specified time that a system is expected to operate without a specified failure event that demands a maintenance intervention, where failure occurrence is to a given level of probability.

3.1.26
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).

3.1.27
performance
A measure of how well an item performs a required function (e.g. the rate at which a valve closes on demand).

3.1.28
probability
A number between zero (0) and one (1) expressing the likelihood that a specific event will occur.

NOTE Probability is usually expressed as the ratio of the number of actual occurrences to the number of possible occurrences.

3.1.29
process
An arrangement of tasks directed toward a specific objective.

3.1.30
production availability
The ratio of actual production to a reference (e.g. planned) production level over a specified period of time.

3.1.31
qualification
The process of confirming, by examination and provision of evidence, that equipment meets specified requirements for the intended use.

3.1.32
redundancy
Existence of more than one means to perform a required function (e.g. by duplicating items).

NOTE Redundancy is one means of achieving fault tolerance.

3.1.33
reliability
The ability of an item to perform a required function, under given conditions of production, environment, and usage, for a required time interval.

NOTE The term “ability” is often interpreted as probability.

3.1.34
reliability and maintainability data
RM data
Data collected to support analysis of reliability, maintainability, and availability of systems.

NOTE Reliability and maintainability (RM) data is the term applied by ISO 14224. ISO 20815 refers to reliability data instead.

3.1.35
risk
The potential for the realization of unwanted, negative consequences of an event.

NOTE Risk may be measured in several ways (e.g. as the probability of occurrence of an unwanted event during a given time or as the product of the frequency of occurrence of an adverse event and a numeric measure of the consequences of the event).

3.1.36
specification
The document in which function, performance, design, and operating requirements are defined, together with associated reliability and integrity goals and requirements.

3.1.37
system availability
The ratio of time a system is functional or in a functional state (uptime) to the total time it is required or expected to function.

NOTE System availability can be specified at field system, package, or subsystem level.

3.1.38
technical risk
Risk associated with the achievement of a technical goal, criterion, or objective that applies to undesired consequences related to technical performance, human safety, mission assets, or environment.

3.1.39
uncertainty
A state of having limited knowledge where it is impossible to exactly describe the existing state or future outcome(s).

3.1.40
uptime
The time interval during which an item is functional.

3.1.41
validation
Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled.

NOTE 1 The term “validated” is used to designate the corresponding status.

NOTE 2 The “use or application” conditions for validation can be real or simulated.

3.1.42
verification
Confirmation, through provision of objective evidence, that specified requirements have been fulfilled.

NOTE 1 The term “verified” is used to designate the corresponding status.

NOTE 2 Confirmation can comprise activities such as:

— performing alternative calculations;

— comparing a new design specification with a similar proven design specification;

— undertaking tests and demonstrations; and

— reviewing documents prior to issue.

3.2 Acronyms and Abbreviations

For the purposes of this document, the following acronyms and abbreviations apply.

ALT	accelerated life testing
AUV	autonomous underwater vehicle
BOP	blowout preventer
CAPEX	capital expenditure
CCFA	common cause failure analysis
CFD	computational fluid dynamics
CM	configuration management
CP	cathodic protection
CRO	control room operator
DfRI	design for reliability and integrity
DPIEF	define, plan, implement, evaluate, and feedback
EC	eddy current
ESDV	emergency shutdown valve
ETA	event tree analysis
FAT	factory acceptance test
FEA	finite element analysis
FEED	front-end engineering design
FFOP	failure-free operating period
FMECA	failure modes, effects, and criticality analysis
FRACAS	failure reporting and corrective action system
FTA	fault tree analysis
GOR	gas-oil ratio
HALT	highly accelerated life test(ing)
HASS	highly accelerated stress screening
HAZID	hazard identification
HAZOP	hazard and operability study
HIPPS	high integrity pressure protection system

HISC	hydrogen-induced stress corrosion cracking
HP	high-pressure
HPU	hydraulic power unit
ILI	in-line inspection
IM-FMECA	integrity management failure modes, effects, and criticality analysis
ITMM	inspection, testing, monitoring, and maintenance
KP	key process
LCC	life cycle cost
LMRP	lower marine riser package
LP	low-pressure
MATIC	manufacture, assembly, testing, installation, and commissioning
MBS	multibeam sonar
MCS	Monte Carlo simulation
MFL	magnetic flux leakage
MFOP	maintenance-free operating period
MOC	management of change
MTBF	mean time between failure
MTTF	mean time to failure
MTTR	mean time to repair
NPV	net present value
OEM	original equipment manufacturer
OPEX	operating expenditure
OREDA	offshore reliability data
PARLOC	pipeline and riser loss of containment
P-FMECA	process failure modes, effects, and criticality analysis
PRM	project risk management
PRS-FMECA	preparedness response scheme failure modes, effects, and criticality analysis
QA	quality assurance
QC	quality control
Q-FMECA	qualification failure modes, effects, and criticality analysis

RAM	reliability, availability, and maintainability
RBD	reliability block diagram
RBI	Risk-based Inspection
RCA	root cause (failure) analysis
RCFA	root cause failure analysis
RCM	reliability centered maintenance
RCMM	reliability capability maturity model
R&D	research and development
RDT	reliability demonstration testing
RIAD	reliability and integrity assurance document
RIM	reliability and integrity management
RM	reliability and maintainability
ROTV	remotely operated towed vehicle
ROV	remotely operated vehicle
SCC	stress corrosion cracking
SCM	subsea control module
SIL	safety integrity level
SIT	system integration test
SOL	safe operating limit
SQP	standard qualification program
SSIV	subsea isolation valve
SSS	side-scan sonar
TQP	technology qualification program
TRAR	technical risk assurance review
TRC	technical risk categorization
TRL	technology readiness level
USV	underwater safety valve
UT	ultrasonic transducer

4 Document Outline and Application

4.1 General

Users of this RP should gain a better understanding on how to manage an appropriate level of reliability and integrity though the life cycle of their systems. Industry-wide users should be able to:

— recognize the trade-off between upfront reliability, integrity, and engineering effort vs. operational integrity management and maintenance effort;

— effectively manage and respond to regulatory requirements or guidance (see API 75) related to or affecting subsea equipment reliability and integrity performance;

— provide better assurance of future reliability and integrity performance of subsea systems;

— effectively manage the risks from using novel equipment (including standard equipment in novel applications) and standard equipment;

— schedule projects and operational activities, including maintenance and intervention, with sufficient time to address all the technical risks.

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

Reliability and integrity are best addressed through industry-wide cooperation in terms of best practice, managing failures that occur and the collection and analysis of performance data. This RP aims to provide a common framework and language for developing common understanding and cooperative progress within the subsea oil and gas industry for the specification and demonstration of reliability and integrity achievement.

The achievement of improved subsea equipment availability and integrity 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 and operations to achieve immediate and tangible improvements to system performance.

4.2 Document Road Map

Figure 1 below shows a flow diagram of how the document may be read by different users as well as a brief description of what can be found in each section. Given that some users may be familiar with the First Edition of API 17N, the flow diagram provides an insight into where an experienced user of the document may want to refer, i.e. the annexes. A new reader, however, is recommended to read through the document's main body to understand the philosophy and its application to subsea asset life cycles. Managers may wish to refer to Annex B for guidance on the KPs and preparation for their implementation within a company or project.

NOTE 1 More detailed guidance on technology qualification has been moved from API 17N to API 17Q, Second Edition.

NOTE 2 API 17Q, Second Edition is planned for publication in 2017. Annexes E and F are included in this document to provide interim guidance and will be removed once API 17Q, Second Edition is published. For all references in the text to API 17Q, the reader will need to refer to these annexes until API 17Q is published.

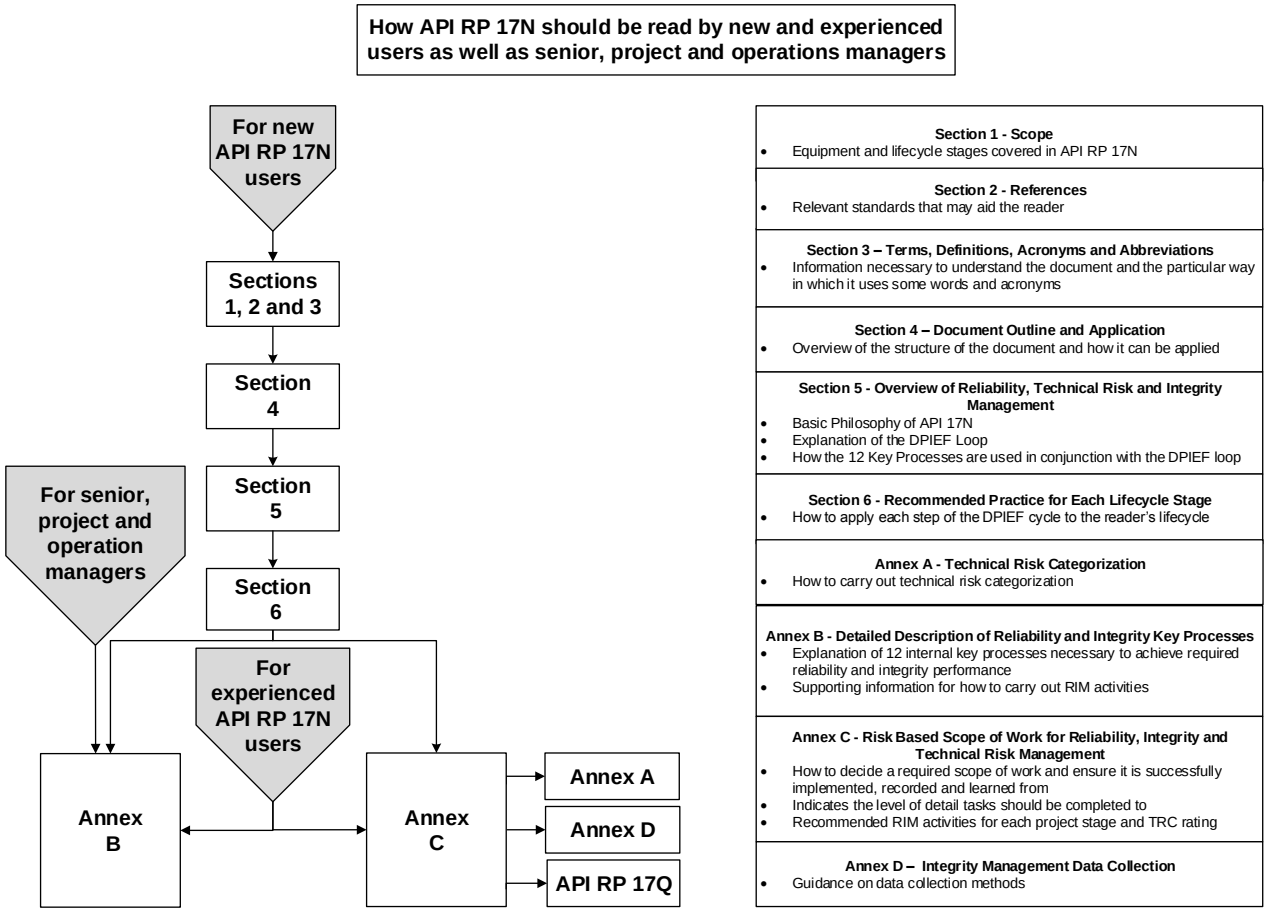


Figure 1—API 17N Road Map

4.3 Project and Operation Applicability

The RP is provided as a guide to RIM for the whole of the subsea industry. It is intended to be applicable to all project scopes and existing assets, including:

— field developments using field proven or fully qualified hardware;

— field upgrades to replace obsolete equipment, extend life of field, or tie back new wells into existing infrastructure;

— new technology development projects;

— field developments in which existing technology is used under extended operating conditions;

— field developments involving new technology.

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

For projects/equipment involving low technical risk (e.g. some projects using field proven or fully qualified hardware), little additional reliability and integrity effort beyond existing good engineering and management practices is expected. However, the guidance within will provide additional considerations for increasing the RIM performance.

4.4 Equipment Applicability

4.4.1 General

This RP applies to all subsea equipment, including:

— subsea equipment and hardware, including related control systems;

— installation facilities and tools;

— system interfaces (e.g. chemical injection interface with a production system);

— subsea intervention and maintenance.

4.4.2 Subsea Equipment and Hardware

From the sand face downhole to the top of the riser, plus the hydraulic power unit (HPU)/master control station (and other subsea-specific surface equipment) and typically including wellheads (both subsea and mud line casing suspension systems) and trees; pipelines, jumpers, flowlines, and end connections; processing equipment; controls, control lines, and control fluids; instrumentation; templates; and manifolds and production (including water injection) risers (both rigid and flexible).

4.4.3 Installation Facilities and Tools

Risks associated with installation facilities, equipment, tools, and procedures should be addressed to ensure that:

— construction, installation, and commissioning procedures will not adversely affect the reliability and integrity of permanently installed equipment;

— unreliability and unavailability performance of required tools and equipment do not impact start-up schedules and hence the production availability.

4.4.4 System Interfaces

Hardware interfacing risks, especially those that also represent boundaries between different organizations, should be identified and addressed.

4.4.5 Subsea Intervention and Maintenance

Considers performance history of the hardware that has been used or can be used to better scope interventions.

Intervention methods, tools, workover, and inspection risks should be addressed such that:

— intervention and maintenance procedures will not adversely affect the reliability and integrity of permanently installed equipment;

— unreliable performance of required tools and equipment do not impact production availability or intervention efficiency.

Although this RP is focused on subsea production equipment, the guidance is generic and may be easily adapted to address the design of subsea hardware used for drilling operations, including the subsea blowout preventer (BOP) and lower marine riser package (LMRP).

4.5 Life Cycle Stages

This RP covers all stages of a subsea system life cycle, including:

— Feasibility;

— concept selection;

— front-end engineering design (FEED);

— detail design;

— manufacture, assembly, testing, installation, and commissioning (MATIC);

— operation;

— decommissioning.

4.6 Company Documentation

Figure 2 shows a typical example of a document hierarchy that may be used for the implementation of reliability, technical risk, and integrity management within a company. The diagram shows a high-level strategy document communicating company intent. This should refer to high-level technical practice documents addressing requirements for projects and operations. Together these documents set out the roles and responsibilities of individuals and groups within project and operation teams.

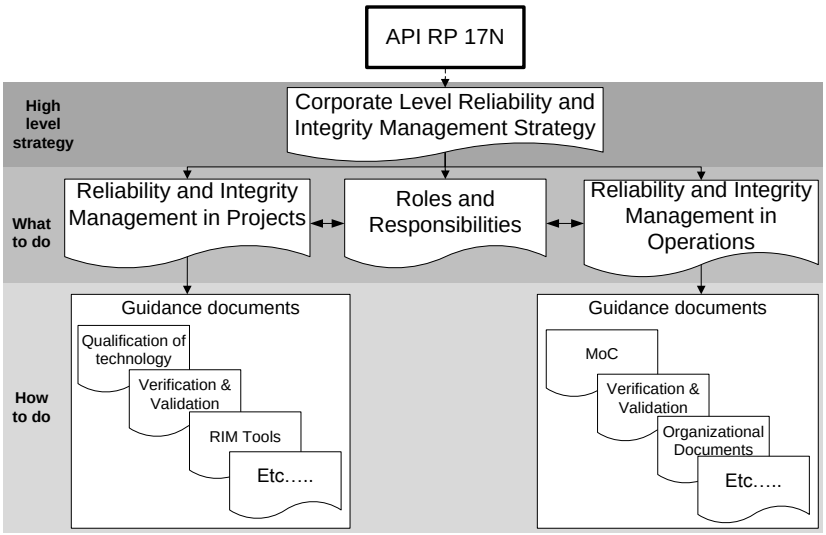


Figure 2—How API 17N Applies to a Company's Reliability, Technical Risk, and Integrity Management Documentation

The technical practice documents are typically supported by a series of guidance notes and/or manuals that contain detailed information on how to carry out tasks identified by the project or operations teams in order to achieve the required levels of reliability, technical risk, and integrity. Individual documents would also contain guidance on KP implementation, though some of these may well have wider applicability than reliability, technical risk, and integrity management and therefore need input from other teams within the company.

API 17N provides guidance on developing an appropriate framework for companies to establish their reliability, technical risk, and integrity management strategy.

5 Overview of Reliability, Technical Risk, and Integrity Management

5.1 General

This section summarizes the basic philosophy behind this RP and explains the reliability and integrity assurance loop (DPIEF loop; see Figure 3) that is the basis behind all the RIM activities described in this document, where DPIEF stands for:

— define;

— plan;

— implement;

— evaluate;

— feedback.

This assurance loop is applied at each life cycle stage of the subsea system (see Section 6 and Annex C):

— feasibility (see 6.5 and C.2);

— concept selection (see 6.5 and C.3);

— FEED (see 6.5 and 6.4);

— detailed design (see 6.5 and C.5);

— MATIC (see 6.6 and C.6);

— operations (see 6.7, C.7, and C.8);

— decommissioning (see 6.10).

Early life stages of field development projects are focused on operator-led activities with involvement from engineering contractors increasing as the project progresses. Supplier activities are generally introduced during FEED and continue during detailed design and MATIC.

5.2 Underlying Philosophy

API 17N is based on the 12 “key” RIM processes listed in 5.9 and described in detail in Annex B. These processes, if adopted, can provide an organization with the basis for a well-organized and rigorous system for the management of reliability, technical risk, and integrity.

The underlying philosophy is based on a belief that:

— the achievement of system reliability and integrity will add value to a field development through maximization of equipment reliability, minimization of intervention for maintenance or replacement of failed equipment, and by preventing events that may cause harm to people or damage the environment;

— the achievement of equipment reliability, integrity, and system availability is primarily founded on the implementation of good reliability and technical risk management practices formally integrated with good subsea engineering using the best available analytical tools and techniques to inform engineering decisions throughout the project life cycle;

— reliability and integrity are core business values that companies are seeking to achieve.

Senior management should ensure that the framework followed adheres to company policy, core company values, and statutory and regulatory requirements and that appropriate levels of authority for decision-making have been agreed.

For practical purposes, the 12 KPs are implemented as a number of integrated RIM activities.

The core activities in the reliability and integrity assurance cycle are comprised of the five basic activities illustrated in Figure 3. These activities are applied during each stage of a subsea system's life cycle and encourage a "stop and think" approach such that:

— clear objectives are set for the work;

— appropriate activities are selected that will meet the objectives;

— there are sufficient time and resources to carry out the activities and analyze results;

— there is confirmation that the activities have been completed correctly and fully evaluated and audited;

— evidence is collated and documented to provide reliability and integrity assurance;

— lessons are learned to improve future asset design, delivery, and operation.

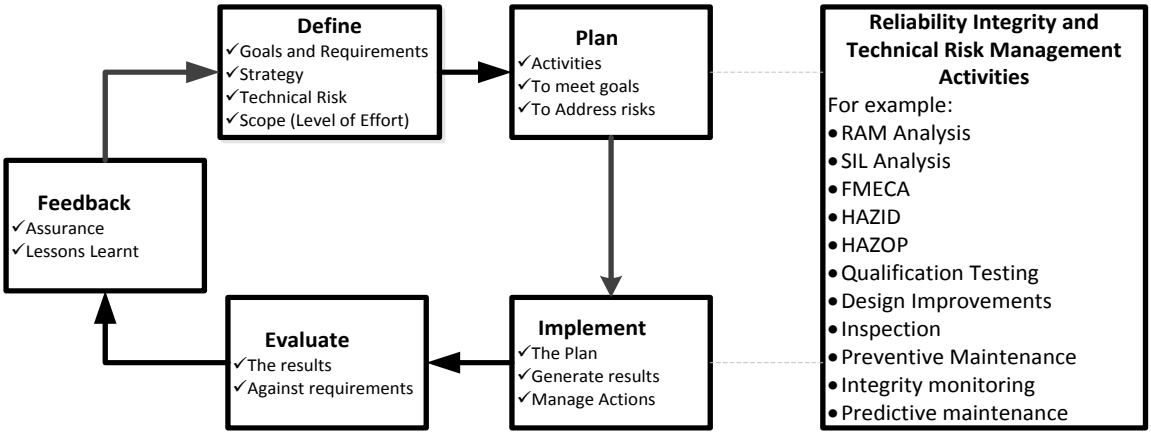


Figure 3—DPIEF Reliability and Integrity Assurance Cycle

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

5.3 Assessment and Management of Risk

5.3.1 General

The assessment and management of risk is fundamentally important to integrity management and also supports achievement of production availability requirements. Identification of risk should include health, safety, financial, environmental, and reputational effects.

The key elements of risk assessment and management are outlined in Figure 4.

NOTE More detailed guidance on risk management is addressed by other standards such as ISO 31000 [2].

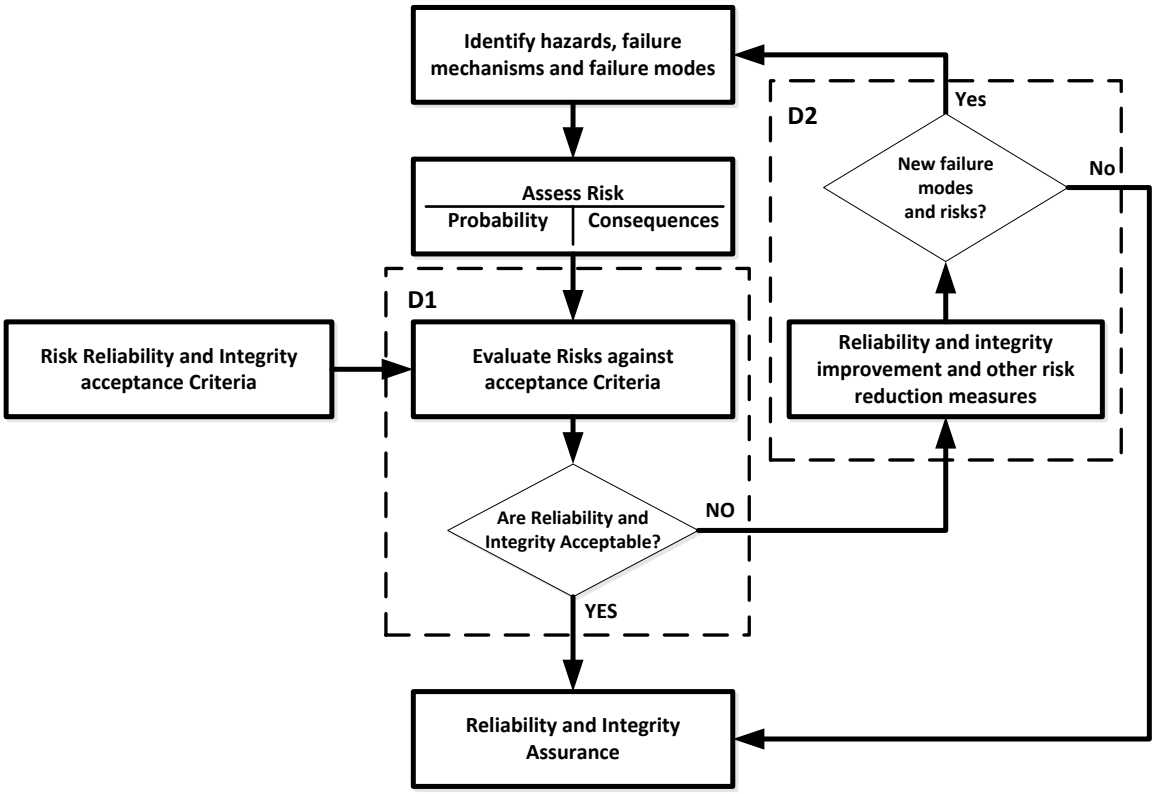


Figure 4—Assessment and Management of Risk

The key elements of risk assessment and management should involve the following.

— Identification of potential failure events and hazards:

  — hazards should include evaluations for hardware, software, the environment, and human error.

— Risk assessment for each hazard, failure mechanism, or failure mode, which will generally involve:

  — estimating the probability of failure events;

  — estimating the consequences of failure should the failure mode or hazard be realized;

  — identification of barriers, mitigation means, and emergency response plans (e.g. using bowtie analysis).

— Evaluation of the risks against risk acceptance criteria set by the company responsible for managing the risk.

— Where the risks are unacceptable, identification of actions to improve reliability and/or integrity and reduce or manage risk.

— Evaluation of the effectiveness of the barriers in place (safeguards and mitigation means).

— Where the risks are acceptable, provide feedback and assurance to senior management, customers, and other stakeholders as needed.

5.3.2 Risk Management Strategies

Possible risk management strategies can typically include:

— eliminate or reduce the probability of hazards, failure modes, and failure mechanisms in design, MATIC, and operations;

— improvements to inherent reliability, reduction of probability of failure through the project life stages;

— detection of the causes of potential failures and taking measures to prevent failures occurring during operations;

— detection and reduction of the likelihood of failures in operation for both the system and operational processes;

— mitigation of consequences should failure be realized;

— development of emergency plan responsiveness.

5.3.3 Key Risk Management Decisions

There are two key decision points (Figure 4) in the management of reliability, integrity, and risk:

— (D1) evaluation of risk against risk acceptance criteria;

— (D2) reliability/integrity improvement and risk reduction.

These together with cost-benefit analysis are the key elements of the evaluate step of the DPIEF assurance cycle (see 5.7).

5.4 Define Step of DPIEF Cycle

5.4.1 General

Define activities should include:

— identification of all required functions, or combination of functions, of an item that is considered necessary to provide a given service;

— accountability and competency of personnel to drive reliability, integrity, and risk management throughout the life cycle;

— input of relevant lessons learned from previous projects and operations;

— identification and categorization of technical risk and uncertainty;

— identification of technology readiness for any new or modified technology to be developed during the project stage and deployed in operations;

— identification of project and operations RIM goals and requirements;

— prioritization of reliability, integrity, and technical risk management effort for the asset.

5.4.2 Input of Lessons Learned

This may be provided as a review document for the project team or as a workshop process involving inputs from experienced engineers [including operations engineers, service provider(s), and supplier(s)] or both. A

company lessons learned database is a useful resource for this activity in addition to service provider(s) and supplier(s) input.

Lessons learned include, but are not limited to:

— process improvements based on previous positive or negative outcomes;

— evaluation of incident reports and corrective actions related to both system and human failures.

5.4.3 Assessment and Categorization of Technical Uncertainty and Risk

The risk assessment effort should be tailored to the level and source of technical uncertainty and risk for the system life cycle stage being considered. Assessments should seek to identify changes from previous projects/assets (change factors) that introduce uncertainty in the ability of the equipment to operate reliably in the field.

The parameters considered as potential sources of uncertainty should include:

— required operating environment (in terms of pressures, temperatures, water depths, production fluids, and seabed conditions, etc.) relative to previous experience;

— the relative novelty of technology to be used in each concept;

— how system configuration deviates from previous practice;

— company and industry experience of using similar systems in similar applications;

— current expected concept reliability and integrity compared with project reliability and integrity goals and requirements;

— how system operations deviate from previous practice.

The tools used for the assessment of technical uncertainty and risk may take different forms during different stages of the life cycle, for example:

— a simple high-level technical review may filter out equipment with technical uncertainty during early design stages such as concept selection and FEED;

— consequence/severity analysis can be used to identify equipment with the greatest impact on production or safety and environment;

— assessment of the potential causes of failure, the consequences of potential failure and the likelihood for each failure [e.g. by integrity management failure modes, effects, and criticality analysis (IM-FMECA), root cause (failure) analysis (RCA), process FMECA (P-FMECA)];

— human factors evaluations can identify sources of human error from FEED through to decommissioning and can identify the possible effect of those errors on reliability and integrity;

— technical risk reviews can be used to identify where equipment is being designed beyond current experience.

The technical risk and uncertainty categorization tool recommended by this RP is described in Annex A. This also provides an indication of the level of RIM effort that may be required by the project/operations team to manage the technical risk and uncertainties.

5.4.4 Goals and Requirements

It is important for the project and operations teams to be clear on what they and the asset are aiming to achieve and why. This includes:

— production requirements, i.e. the ability to maintain uptime and minimize downtime;

— integrity requirements, i.e. the ability to contain production fluids, isolate equipment, and remain fit for purpose over the life cycle of the system, while protecting safety, health, and environment;

— risk acceptance criteria, i.e. the limit of acceptable or tolerable risk.

Goals identify the reliability performance the project team **would like to achieve**.

NOTE It is unlikely that integrity goals will be defined for a project as these are more likely to be defined as regulatory requirements.

Requirements identify the reliability and integrity performance that the asset is required to achieve in order to meet the business and regulatory objectives.

Reliability and integrity goals and requirements should be:

— consistent with company and/or client business requirements for production, safety, and environment;

— used to drive the design and system developments;

— fully supported by senior management, project teams, operations teams, vendors, and contractors.

Goals and requirements may be expressed in words (qualitative) or numerically (quantitative); see B.3.

At each life cycle stage, the overall project goals and requirements should be reviewed and verified by the project and operations teams.

The level of equipment (project, package, subsystem, etc.) that the goals and requirements are applied to should be developed in line with the life cycle stage as summarized in 6.3.

5.4.5 Strategy to Be Used

The strategy is the general approach the project and operations teams will take to achieve the stated goals and requirements in a way that adds value to the asset.

— **Reliability Strategy.** Achieve a required level of performance or system availability by extending the life of equipment before failure or maintenance.

— **Maintainability Strategy.** Achieve a required level of performance or system availability, for example by minimizing the time to restore failed equipment to an operable state.

— **Standardization Strategy.** Achieve acceptable reliability and integrity through use of field proven or standard equipment as far as practicable.

— **Risk Mitigation Strategy.** Use operational mitigations, such as spare capacity and rapid intervention responses, to reduce the effects of system failure and human error.

— **Integrity Strategy.** Identify the processes (barriers and means of mitigation) that will be instituted to maintain integrity during operations (i.e. the integrity management processes).

— **Obsolescence Strategy.** Identify equipment that are likely to become obsolete within the life cycle of the asset and develop an obsolescence management plan.

There will inevitably be a trade-off between different strategies to achieve the overall goals and requirements set. An example of such a trade-off for a high integrity pressure protection system (HIPPS) system would be that between integrity (fail-safe) and production availability and how this impacts the design process.

This RP recommends implementing a reliability, integrity, and technical risk management program or incorporating the essential elements of such a program into a broader project and asset management program, which has the ability to address some, or all, of the above.

5.4.6 Identification of Scope of Work

The scope of work for any given life cycle stage is the list of activities that will address the identified technical risks and the specified goals and requirements for the equipment with the system scope. This may include, but is not limited to:

— system production availability analysis to determine the extent to which design configurations meet economic production targets;

— system reliability and integrity assessments to identify the probability of system failures (e.g. failure of the chemical injection system, the probability of failing to shut-in a well, shutdown a complete system or start up a system, etc.);

— consequence/severity analysis to identify critical systems;

— FMECA to identify and, where practicable, design out potential failure modes;

— obsolescence assessments to identify equipment that may become obsolete during the field life;

— safety integrity level (SIL) assessments for safety critical subsea equipment (e.g. HIPPS);

— design reviews to expose equipment and systems at various stages of design to the opinion of subject matter experts;

— testing and analysis to develop understanding of and demonstrate potential for functionality and reliability;

— reliability centered maintenance (RCM) to develop a robust subsea maintenance and integrity management system during operation;

— defining processes to be implemented for life of field to assure integrity, such as Risk-based Inspection (RBI) processes;

— human error assessment [e.g. as part of hazard and operability study (HAZOP);

— hazard identification (HAZID), or P-FMECA] to evaluate design, manufacturing, and operational processes for the likelihood of human errors and to identify means of mitigating the potential for error. For more information on human error evaluation, see Reference [3].

All activities should:

— be appropriate for the level of risk identified;

— be realistically achievable within the time frame of the wider project schedule;

— add value to the project;

— be cost effective;

— be consistent with the project goals, requirements, and strategy;

— include input from relevant departments involved with the product’s life cycle.

5.5 Plan Step of DPIEF Cycle

The RIM plan establishes the detail of how the scope of work is to be accomplished. A plan should be developed for each stage in the subsea life cycle and should cover such areas as:

— the specific activities to be carried out (analyses, assessments, reviews, etc.);

— resources to be used (people, software/hardware tools, etc.) and time period that each resource is required;

— roles, responsibilities, and accountability for all personnel involved at all relevant management levels;

— deliverables for each activity;

— any requirements for verification and validation;

— schedules and milestones.

As projects proceed the organizations involved will change, for example when suppliers are selected and at project handover to operations. The RIM plan should clarify which organization will do what, within each activity, in terms of:

— specifying requirements;

— completing the work;

— verifying that the work meets the requirements;

— identifying physical and organizational interfaces.

The plan should only contain what is achievable within the 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).

5.6 Implement Step of the DPIEF Cycle

The process of implementing the activities at each life cycle stage should include the following activities:

— breaking down the plan into a series of tasks or actions;

— tracking and close out of plans to ensure completion;

— verification and checking against stated goals and requirements to provide assurance that the identified technical risk has been addressed to a sufficient degree for the project stage.

Implementation of the plan is supported, through the application of good management practices as described by the KPs in Annex B.

Throughout the life cycle, implementation activities are intended to provide assurance that:

— potential failure modes that could affect system performance have been analyzed and managed;

— all design decisions are consistent with the reliability, availability, maintainability, and integrity goals and requirements;

— qualification of equipment has addressed function, performance, reliability, integrity, integrity manageability, and maintainability required by the business and is at an acceptable level of progress to proceed to the subsequent life cycle stage;

— all identified lessons learned from previous projects and operations have been incorporated;

— the supply chain is fully integrated into the reliability, integrity, and technical risk management program;

— the achieved reliability, availability, maintainability, and integrity performance will allow production, financial, and company performance goals and requirements to be met.

5.7 Evaluate Step of the DPIEF Cycle

As the plans are implemented and results are delivered at each life cycle stage, they should be analyzed and evaluated against the specified goals and requirements and risk acceptance criteria (see Figure 4) to identify actions for the next stage in the life cycle, and for management of emergent risk, for example:

— evaluation of reliability, availability, and maintainability (RAM) analysis results against performance availability objectives to select best design configuration at concept selection stage;

— evaluation of results from qualification tests and activities during FEED and detailed design for new technologies to be used in the project against acceptance criteria;

— evaluation of inspection and integrity monitoring results during operation against acceptance criteria;

— evaluation of residual risks that cannot be completely eliminated;

— evaluation of the capability of a company to manage reliability and integrity in a project or operations [e.g. using a reliability capability maturity model (RCMM) audit; B.12.4.2].

Risk acceptance criteria used by the project team should be agreed with the operations team and be in line with overall business policy. The method of risk evaluation and associated risk matrix should be consistent throughout the life cycle.

The technical risk categorization (TRC) level should be revisited to identify changes to the original assessment arising from any new information as the design evolves. New technical risks generally require additional action management; these risks should be addressed and managed through appropriate strategies to meet defined risk acceptance criteria (discussed in 5.3.2).

5.8 Feedback Step of the DPIEF Cycle

5.8.1 General

The feedback step should include:

— feedback of lessons learned;

— operator’s technical risk assurance review (TRAR);

— reliability and integrity assurance documentation (RIAD).

For all life cycle stages, the feedback and assurance step is used to provide documented evidence to:

— support decision-making at each life cycle stage (e.g. as part of the decision support package);

— assist other projects at earlier stages.

5.8.2 Lessons Learned Feedback

A review of the work done may include a review to identify and record any lessons learned that may be of value to future projects, such as:

— technical risks, failures, or unwanted events that were not anticipated, but could have been;

— risks that were overestimated and why;

— successes that can be applied to other projects (opportunities);

— suggested improvements on how to complete specific activities (resource, processes, schedule, etc.);

— results of audits.

Feedback aims to capture and distribute lessons learned such that they are usefully utilized. A key interface is that between the project team and the operations team. Important lessons learned in operations should be communicated to future project teams to enable operational reliability and integrity experience to be an input to the design process.

5.8.3 Operator's TRAR

TRARs may be used by an operator to identify any residual risks that may have been overlooked or insufficiently addressed by an equipment vendor's risk assessments.

Reviews should be performed for equipment with high levels of technical risk:

— new technology;

— equipment undergoing major design changes or major changes in operations;

— high-level reviews are performed at the end of FEED before detailed design;

— detailed reviews are performed toward the end of detailed design before manufacture.

5.8.4 RIAD

Throughout the life cycle, typically at the end of each life cycle stage, a documented record should be produced. The RIAD should cover:

— activities performed and completed;

— evidence in the form of a summary of results with links, as appropriate, to detailed reports;

— key findings from studies performed (e.g. testing and analyses);

— decisions made and implemented measures;

— claims related to the reliability and integrity goals and requirements;

— assurance that the technical risks identified for each package can be managed within the project schedule and budget.

The RIAD provides documented assurance that the technical risks and uncertainties have been addressed.

Assurance claims should only be based on the evidence reported in the RIAD and should clearly outline the extent to which reliability and integrity goals and requirements have been met.

5.9 KPs for RIM

There are 12 organizational KPs that support delivery of reliability and integrity and implementation of the DPIEF cycle. 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 that promote good reliability, integrity, and risk management practice.

The relationship between the DPIEF cycle and the 12 KPs is shown in Figure 5.

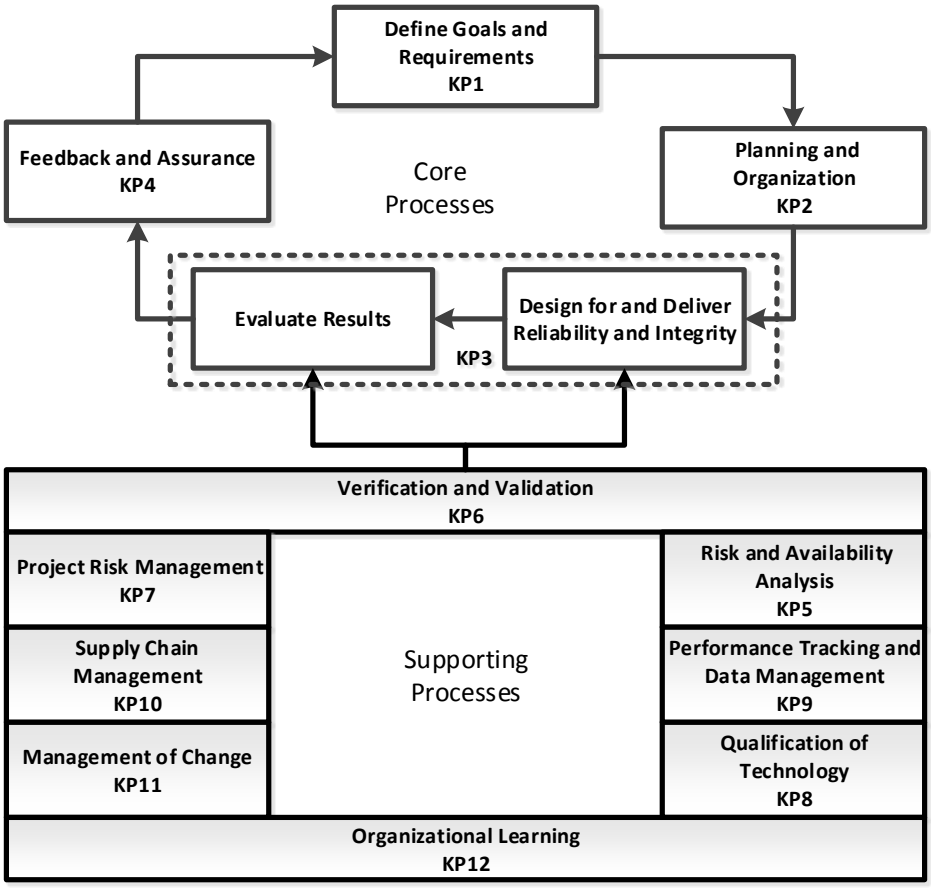


Figure 5—KPs for RIM

KP 1—Define Goals and Requirements ensures that the project and operational goals and requirements are fully aligned with overall business performance and regulatory objectives and provides the focus for delivery of reliability and integrity assurance.

Table 1—Operator Business Requirements and Reliability/Integrity Implications

Operator Business Requirements	RIM Focus
High production availability	Reliability: maximize uptime
	Maintainability: minimize downtime
Best value field development	Maximize production
	Minimize operational expenditure (OPEX)
High level of integrity assurance	Containment: low probability of loss of containment
	Isolation: low probability of failure on demand

The trade-off between the purchase cost and the operational expenditure should be formally recognized when considering the need for reliability and maintainability improvement (see B.3 for more details). Requirements related to the trade-off between automated design and human operational processes need to be assessed to evaluate the risks of human error compared to a more complex design.

Each organization should clearly define the authority level at which goals and requirements need to be agreed.

KP 2—Planning and Organization allocates leadership and resources to the required RIM activities such that they add value to the asset overall and do not adversely impact on schedule requirements. The activities identified should be considered an integral part of the engineering process and integrated with conventional engineering tasks in the project/asset management system. The right resources are identified for detection and correction/mitigation of issues throughout the cycle (see B.4 for more details).

KP 3—Design for and Deliver Reliability and Integrity is the key process for delivering reliability and integrity of subsea installations (see B.5 for more details). Information gathered from reliability and integrity assessment activities should be evaluated during the design process to drive the design's ability to achieve and deliver the specified availability and integrity requirements. Decisions on what actions to take require a good understanding of both failure mechanisms and how inappropriate actions taken during the design, manufacture, assembly, test, and installation phases contribute to failure in operation.

KP 4—Feedback and Assurance is the process of communicating the information pertaining to reliability, integrity, and technical effectiveness of the system to other members of a project/operations team and to senior management. The key output from the reliability and integrity assurance process is the RIAD (see B.6 for more details).

KP 5—Risk and Availability Analysis provides RIM 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 (this will depend on the life cycle 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.7 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.8 for more details).

KP 7—Project Risk Management (PRM) addresses nontechnical budget and technical risks throughout the project life cycle (or field upgrades during operations) to enable all risks to be identified, quantified, managed, and preferably eliminated (see B.9 for more details).

KP 8—Qualification of Technology 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 (see B.10 for more details).

KP 9—Performance Tracking and Data Management collects and organizes reliability and integrity performance data from all life cycle stages of every subsea asset to support asset management and the assessment of reliability, integrity, availability, and production efficiency (see B.11 for more details).

KP 10—Supply Chain Management plans, manages, and adds efficiency and value during planning, sourcing, procurement, conversion, and logistics management activities. Supply chain management ensures that reliability, integrity, obsolescence risks, and technical risk management goals, requirements, achievements, and lessons learned are communicated within and between all organizations (including all suppliers) involved in the life cycle (see B.12 for more details).

KP 11—Management of Change (MOC) ensures that any changes in the project (to scope, design, plan, process, etc.) or in operations (procedures, remedial intervention, field upgrades) are consistent with the

reliability, integrity obsolescence risk, and technical risk management goals and requirements. It also ensures that the change and impacts are fully assessed and managed (see B.13 for more details).

KP 12—Organizational Learning provides a common framework to capture an organization's learnings over an asset's life cycle and communicate them back into the organization to be adopted by later projects and operations teams. The lessons learned usually cover the whole life of the asset from strategic thinking and decision-making, through project execution and asset operation and should include both good and bad practice (see B.14 for more details).

These KPs provide a supporting environment for the reliability, integrity, and risk management activities. When the appropriate process is identified, further information and guidance is available within Annex B. When these processes are implemented across an organization, the reliability, integrity, and technical risk management effort for each subsea system is reduced (good practice that otherwise had to be specified now happens automatically).

Figure 6 provides a summary of the life cycle stages for which different KPs are relevant or may be relevant under some circumstances.

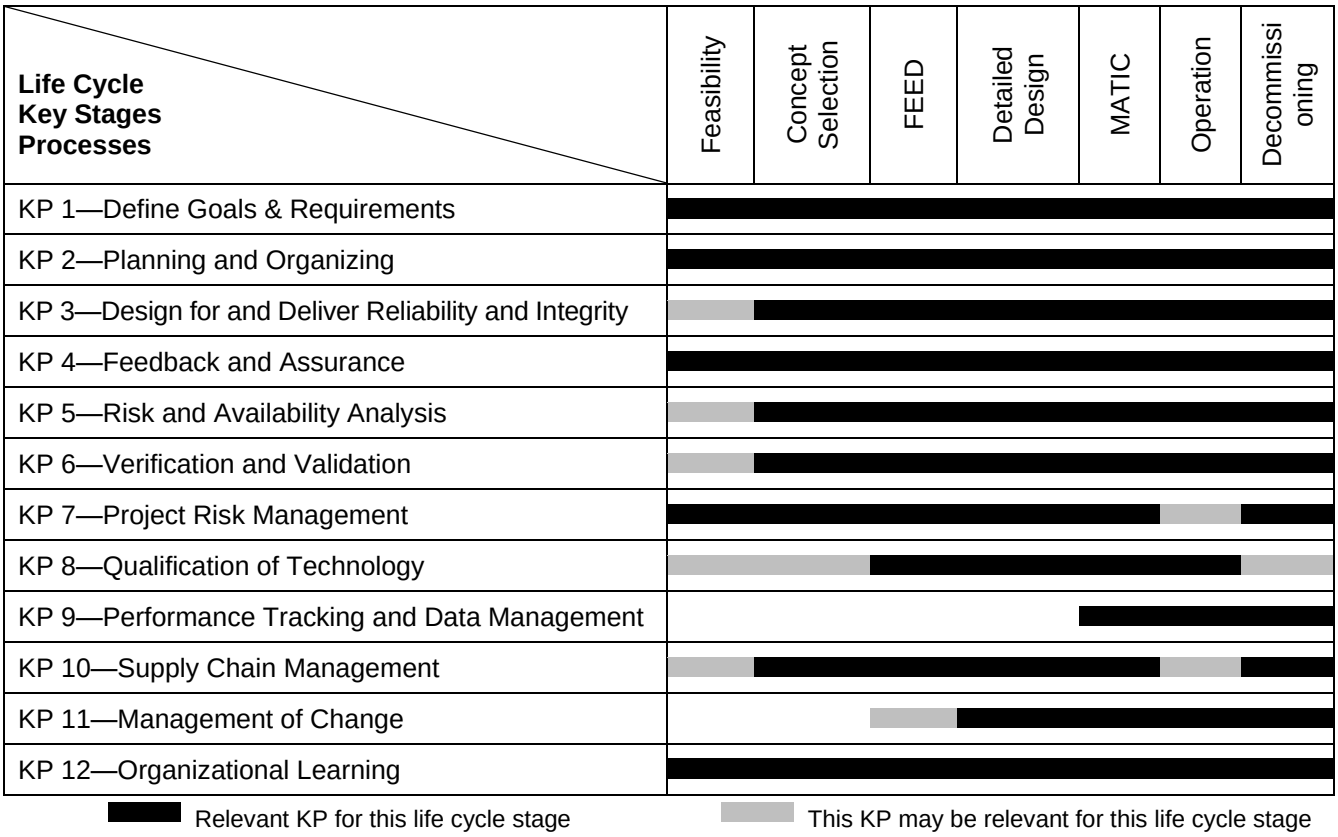


Figure 6—Summary of the Life Cycle

6 Recommended Practice for Each Life Cycle Stage

6.1 General

This section provides a general approach to achieve the desired reliability, integrity, and risk management performance at each stage of the subsea asset life cycle. Further details are provided in Annex C.

6.2 Configuration Management (CM)

CM is not formally addressed in this RP as a separate process. However, the main key elements of a CM process are captured in the current 12 KPs (see Annex B).

CM is a system engineering process that embodies rules, procedures, techniques, methodology, and resources to assure that:

— the configuration of the system and/or item (its physical and performance attributes) are fully documented;

— changes made to any item during design, MATIC, operations, and decommissioning are beneficial and are implemented without adverse consequences;

— changes are managed until incorporated in all affected items.

NOTE Many companies may already have CM as a defined process that can be integrated with the recommendations in this RP. For more information on CM, see Bibliographic Items [4], [5], and [6].

6.3 Application of the DPIEF Assurance Cycle

The life cycle of a subsea system involves a number of stages through which the system is developed and operated. As the life cycle progresses, the subsea system becomes better defined and the focus of the DPIEF cycle at each stage (see Table 2) should change accordingly.

The activities during the project stages of the life cycle are focused on designing-in reliability, integrity, and their manageability. During operations, the focus is on integrity management, production availability, data collection, and understanding root causes of failure. Importantly, operations teams should input into project activities during the design life cycle to ensure operational aspects are addressed.

Table 2—Project and Asset Life Cycle Focus and Considerations

Life Cycle Stage	Focus	Considerations
Feasibility	Project-level view	Considers the overall system challenges to project performance (location, environment, new technology, resources).
Concept Selection	System-level view	Considers the reliability, integrity, and risk implications of technology and operational processes for the 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, human error), including reliability, integrity, and integrity management requirements.
Detailed Design	Subassembly- and component-level view	Considers the reliability and integrity risks associated with individual components (e.g. gate valves, connectors, sensors).
Manufacture, Assembly, Testing, Installation, Commissioning	Procedural-level view	Considers how procedural control can be used to prevent errors and the introduction of defects that can reduce reliability and integrity performance of the equipment after manufacture. This also includes collecting performance data during testing and installation to improve future projects.
Operations	Procedural-, system-, and component-level view	Considers how procedural control can be used to prevent errors and equipment failures affecting system reliability and integrity performance throughout operations, including interventions. This includes measuring and maintaining actual performance data and taking actions to continuously improve future performance.
Decommissioning	Procedural- and component-level view	Considers how procedural control can be used to prevent errors affecting integrity performance for the decommissioning process. This may also consider the reliability and integrity of components given increasing demand for reuse.

This RP recommends adopting the approach in Figure 7 to apply the DPIEF assurance cycle to the different life cycle stages.

The “double DPIEF loop” shown in operations, is included due to the repetition of the “normal operations loop” (right-hand side loop). Design, by comparison, proceeds iteratively from start to end (at commissioning/hand-over). It is therefore necessary to include a separate “corrective action loop” (left-hand side) within the operations stage to clearly distinguish between normal operations and corrective action.

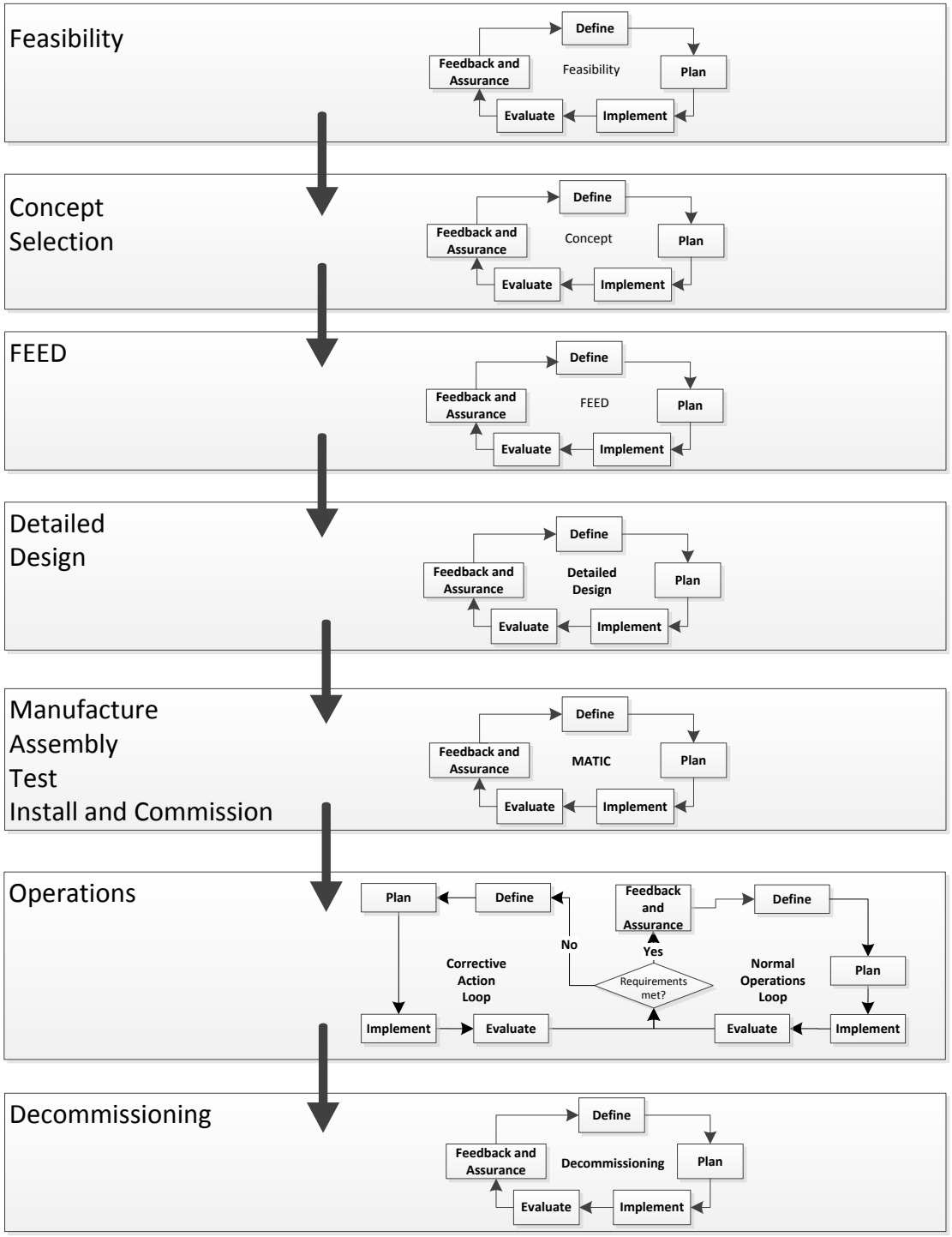


Figure 7—Application of DPIEF Cycle to the Subsea System Life Cycle

The level of RIM effort associated with the reliability, integrity, and risk management activities at each life cycle stage should be consistent with the level of risk identified for the given subsea system and field. This RP recommends the use of TRC for identifying the level of risk and uncertainty (see Annex A).

NOTE Other industry standards (e.g. DNV-RP-A203) use alternative risk categorization and novelty assessment schemes and may be used by some organizations instead of TRC.

Annex C provides specific guidance on application of the DPIEF cycle at each life cycle stage. However, the specific activities required (e.g. application of system reliability analysis) may depend on both the level and source of technical risk as identified by the TRC. Annex C also provides additional guidance on recommended activities at each life cycle stage depending on the risk category.

Regardless of technical risk, there are four activities and associated documentation that should be continuously updated throughout the life cycle and are an integral part of implementation of the DPIEF assurance cycle:

— TRC;

— technology readiness level (TRL);

— statement of goals and requirements;

— RIAD.

In order to achieve consistent outcomes across all projects and assets, organizations should create a generic scope of work for each life cycle stage for each technical risk category. This should then be refined to make a specific scope for the project/asset application.

6.4 Timing of the DPIEF Loop in the Asset Life Cycle

The DPIEF loop is applied at every stage of the asset life cycle; however, the actual time at which a team may initiate activities relevant to a stage will vary. For example, the operations team may usefully initiate definition of operational requirements by providing input to the project team as early as concept selection (see Figure 8).

6.5 Design Stages

From a reliability and integrity perspective, the intent during the design stages may be summarized as:

— create the required inherent reliability, availability, maintainability, and integrity in the design;

— provide evidence of the above through analysis, testing and use of historical performance data.

Annex C provides detailed guidance of RIM activities appropriate for each design stage of the life cycle as indicated in Figure 8.

6.6 Manufacture, Assembly, Testing, Installation, and Commissioning (MATIC)

From a subsea reliability and integrity perspective, the intent during the MATIC stages is to:

— ensure that the levels of reliability, availability, maintainability, and integrity designed into the subsea production system are not compromised by the MATIC activities;

— that any nonconformances, system faults, or human errors in the design itself or introduced during the MATIC stages are identified and corrected. Ideally these should be implemented and managed before production start-up or as soon as possible thereafter.

Section C.6 provides detailed guidance of RIM activities appropriate for the MATIC stage.

		Feasibility	Concept Selection	FEED	Detailed Design	Manufacture Assembly Testing	Installation Commiss-ioining	Operations	Decommi-ssioning
Feasibility (See C.2)	D								
	P								
	I								
	E								
	F								
Concept Selection (See C.3)	D								
	P								
	I								
	E								
	F								
FEED (See C.4)	D								
	P								
	I								
	E								
	F								
Detailed Design (See C.5)	D								
	P								
	I								
	E								
	F								
Manufacture, Assembly, and Testing (See C.6)	D								
	P								
	I								
	E								
	F								
Installation and Commissioning (See C.6)	D								
	P								
	I								
	E								
	F								
Operations (See C.7 and C.8)	D								
	P								
	I								
	E								
	F								
Decommissioning (See 6.10)	D								
	P								
	I								
	E								
	F								

Figure 8—The Relative Time in the Asset Life Cycle That Each Stage of the DPIEF Loop Should Be Applied

6.7 Operations

6.7.1 General

From a reliability and integrity perspective, the intent during the operations stage may be summarized as:

— achieve and sustain the level of reliability, availability, maintainability, and integrity that is inherent in the design;

— sustain production without compromising system integrity;

— ensure that equipment reliability and integrity performance do not deteriorate beyond acceptable levels over time;

— provide evidence of the above through in-service inspection, monitoring, testing, and appropriate maintenance and repair or replacement strategies.

Any failures of equipment that lead to loss of production or loss of containment have very significant business consequences once production starts. In addition, there can be health and safety consequences associated with failure mitigation and repair activities. Subsea failures will generally require intervention to repair or replace failed items and the simplest intervention task becomes a difficult and expensive task if it has to be conducted on a subsea facility. Whether the intervention is carried out by diver, remotely operated vehicle (ROV), or wire-line, an expensive, dedicated vessel must mobilize, transit to site, carry out the task, return, and demobilize, so that the "on hire" period is significantly longer than the duration of the actual task. For this reason, it is best to minimize the requirement for intervention on any subsea facility.

6.7.2 Reliability and Integrity Assurance in Operations

6.7.2.1 General

The RIM process for the operations stage is shown schematically in Figure 9. The application of the DPIEF loop to the operations stage includes both a normal operations loop and a corrective action loop. The IM-FMECA is the key tool used to determine the initial inspection, testing, monitoring, and maintenance (ITMM) plan and the subsequent updating of the plan following periodic RIM campaigns.

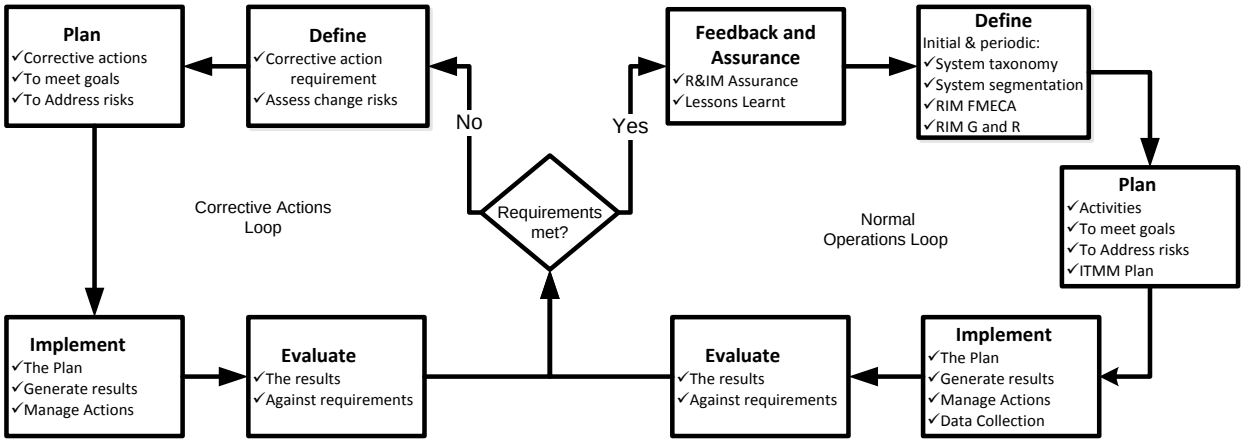


Figure 9—Double DPIEF Loop in Operations

6.7.2.2 Normal Operations Loop

The normal operations DPIEF loop applies to the periodic (typically annual) integrity management campaigns. The define and plan steps for the first iteration of the DPIEF loop should be completed during MATIC stage and handed over to operations. Subsequent iterations and changes to the define and plan stage outputs depend on the results obtained during the implementation of the plan during the integrity management campaigns.

The development of an effective RIM system for operations should be started as early as concept selection with operations personnel being involved in the selection and design process to ensure:

— lessons learned from previous operations are integrated into the design;

— the operations team understand the design assumptions for the system performance and what mitigations or safeguards were accounted for in the design;

— the operations team agrees on risk acceptance criteria with the design team and plays a role in the evaluation stage in projects.

Operations team inputs and interactions should be gradually increased and sustained throughout the design life and through the MATIC stages.

C.7 provides detailed guidance of appropriate RIM activities during normal operations.

6.7.2.3 Corrective Action Loop

The corrective action loop should be initiated whenever significant remedial measures or corrective actions are required. The corrective actions follow their own DPIEF loop and in many cases may be considered as a small project.

The identification and reporting of failures in the normal operations loop and the documentation of corrective actions undertaken in the corrective action loop may be formally integrated into a FRACAS (failure reporting and corrective action system) database. This may be usefully linked to an asset-specific IM-FMECA database.

The corrective action loop is further addressed in C.8.

6.8 Field Upgrades and Field Extensions

Typically field upgrades and extensions, such as a single- or two-well tieback to an existing system, should be considered as small projects. As such they should follow the existing guidance for projects in Annex C.

If the equipment to be installed is similar to existing equipment [e.g. using standard trees and subsea control modules (SCMs) of the same design as the existing system], the level of additional reliability effort should be modest provided that the existing system has already been studied to assess reliability and integrity (e.g. FMECA studies for the particular design of SCM and christmas trees already exist). However, the minimum RIM activities that should be carried out for any field extension are:

— TRC and TRL checks for the additional hardware;

— update RAM analyses to include the extended system architecture;

— update IM-FMECA and preparedness response scheme (PRS)-FMECA to identify any additional spares or integrity management activities or any threats to integrity or reliability related to the new location and the specific environment.

6.9 Life Extensions

As new reservoirs are discovered or new methods are developed to extend the life of existing reservoirs, there is an increasing requirement to extend the operational life of existing offshore installations and subsea infrastructure beyond the original field life. At the end of a system’s design life, although most components and structural items of equipment will have suffered some level of degradation, in many cases, the actual level of degradation will be less than that allowed for at the design stage because most equipment is designed conservatively, with large safety margins. This therefore provides an opportunity for life extension.

The continued operation of equipment beyond field life introduces increased risk of failure and therefore demands particular attention to the management of reliability and integrity through inspection and monitoring of degradation.

Before extending equipment life the following should be undertaken.

— A thorough assessment of the condition of the equipment to be used with particular attention paid to critical systems. This provides the baseline for moving forward into the extended life period.

— Detailed risk assessment of critical systems to identify the risk of failure over the extended period of life. This may include:

  — updates to the existing field IM-FMECA;

  — assessment of the remaining life of critical systems (see NOTE) and its comparison with the extended life required by field business case;

— identification of equipment with insufficient remaining life, which will need to be replaced at the start of, or during the extended life period;

— updates to the ITMM program for all equipment, including updates to the ITMM frequency over the remaining life.

NOTE The assessment of the remaining life of a degrading system or item of equipment may be undertaken as a probabilistic assessment in which an estimate is made of the life at which the probability of failure exceeds the acceptable probability as defined by company or regulatory risk acceptance criteria. Acceptable probability can also be defined in terms of acceptable safety margin (Reference [7]).

ITMM frequencies should be consistent with the increasing failure rate of ageing equipment and structures and with the risk acceptance criteria.

The RIM activities outlined in C.7 and in Annex D may be used to support RIM of life extension work.

6.10 Decommissioning

6.10.1 General

In general, the decommissioning of a field constitutes a project and, as such, the entire process outlined in this RP applies. However, on completion of decommissioning the following specific issues should be addressed.

6.10.2 Feedback of Life Performance

When a field is decommissioned, subsea facilities can (in some geographical areas, have to) be recovered to shore for reuse, recycling, or disposal. As part of this process there is additional value to be gained by providing original equipment manufacturers (OEMs) with access to retrieved items to enable additional learning on long-term equipment performance. This is an opportunity to determine the extent to which components, which were inaccessible on the seabed, were overengineered—i.e. have remaining capacity at end of field life (which may, anyway, exceed design life). This might include:

— measuring wall thickness of components such as manifold headers or valve bodies;

— investigating corrosion/erosion at elbows or tee connections;

— carrying out accelerated testing of solenoids or directional control valves to see how many further cycles are required to failure;

— carrying out electrical testing on, and dissection of, umbilicals and power cables to assess the remaining life;

— assessing polymer degradation in flexible flowlines and risers.

Such investigations will help to define the late end of the “bathtub” curve for a number of components, and may help to reduce the costs associated with overengineering systems.

6.10.3 RIM Review

At decommissioning, the effectiveness of RIM can be reviewed from the whole life perspective. This is an opportunity to determine, in light of the state of the overall system and its components at end of life, what other data, had it been available, would have improved the management of reliability and integrity. Maintainability shortfalls can be documented. It is also an opportunity to review statistics such as mean time between failures, or mean time to repair (MTTR), in terms of variability over field life and to assess reasons so as to produce more reliable data and benchmarks for the future.

6.10.4 Feedback of Costs

Operators are encouraged to capture costs on completion of decommissioning to support future life cycle cost (LCC) assessments, since this is the only time that accurate decommissioning costs can be confirmed. These costs should be put in the context of the extent to which the field life, and reservoir performance, matched original expectations. It is only by accurately cataloguing such data that LCC models can be calibrated and improved.

Annex A
(informative)

Technical Risk Categorization (TRC)

A.1 General

This annex provides an example of one method of categorizing technical risk to enable an appropriate level of reliability, integrity, and risk management activities to be defined at each project stage.

NOTE Other industry standards (e.g. ISO 20815 and DNV-RP-A203) use alternative risk categorization schemes and may be used by some organizations instead of TRC.

A.2 TRC

TRC is common to all project stages of the life cycle (from project categorization in feasibility through to component TRC in detailed design, and tooling/handling and procedural risk categorization during manufacture and installation). It occurs toward the beginning of every project stage and is a qualitative assessment of a number of "change risk" factors that can influence the uncertainty of failure. It is also reviewed toward the end of each project stage as part of the "evaluate" step in the DPIEF assurance cycle.

TRC should be implemented as a formal assessment process structured to ensure consistency across different projects and should:

— consider all sources of technical uncertainty that could impact the ability to achieve required performance using the five "change risk" factors (reliability, technology, architecture/configuration, environment, and organization);

— provide a qualitative "score" of technical uncertainty based on the perceived deviation from previous experience to facilitate prioritization of RIM and technical risk mitigation effort [e.g. the method presented here uses categories A (very high), B (high), C (medium), and D (low)];

— adjust the level of TRC focus from an overall project assessment to a detailed component assessment as the project develops from feasibility to design and manufacture;

— enable assessment of both the subsea equipment and the associated procedures used, for example, during manufacture and installation.

The levels of technical uncertainty for each change risk factor are illustrated against some typical keywords for the design stages (feasibility through to detailed design) in Table A.1 and for tooling and procedures used through the MATIC stages in Table A.2.

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

A.3 Ground Rules

TRC should not be an onerous activity. It is intended to be a high-level review process to help identify priorities. The following ground rules are used to facilitate the TRC process.

— Define the component, package, system, or procedure that the TRC is to be applied to.

— Consider the defined component, package, system or procedure against each change factor using the keywords (in either Table A.1 or Table A.2) as a guide to the types of changes that may affect the TRC for that change factor.

— If there is any doubt as to which technical risk category applies, select the higher category (and investigate the uncertainty). The selected category for each change factor should be accompanied by a

brief explanation/justification of the category to aid future understanding and support identification of appropriate risk management activities.

— The overall TRC for the project, component, package, system, or procedure is the highest of the individual categories for each factor, except where this factor is Organization. In the case of having the highest TRC risk/uncertainty category as Organization, the team carrying out the TRC may address the organizational risks and then reduce the TRC to the highest equipment related category.

— The definitions in Table A.1 and Table A.2 are general and are intended to be applied at project, system, package, component, and procedure levels although some interpretation for each project stage and project scope may be necessary. Detailed project knowledge may supersede the general guidance with recorded justification.

— Once a TRC has been defined for the component, package, system, or procedure, Table A.3 can be used as a template to help define the level of effort that is likely to be required in relation to reliability, integrity, and risk management at each stage of the asset life cycle. Section A.4 has more detail on how to do this.

This categorization activity does not consider criticality—i.e. the consequences associated with potential failure of an item. The recommended level of reliability and integrity effort and scope of work may, therefore, be revised if it does not add value or does not indicate a high enough effort (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).

NOTE "Technical risk" in the context of TRC refers to uncertainty and not the combined effect of probability and consequence (the implied consequence is inability to perform as intended). The recommended level of effort/work scope may be omitted if it is not perceived as cost beneficial/value added based on the severity of the potential failure (similarly greater effort may be necessary where there is high severity associated with the potential failure). It is not recommended that such a cost-benefit screening is applied prior to the TRC activity (i.e. the absolute minimum level of assessment should be the TRC).

A.4 Level of Effort

Table A.3 provides an example for the relative reliability, integrity and risk management effort that is likely to be required at each stage of the asset life cycle for the reader's defined level of technical risk and uncertainty. This type of table can be filled in by the person/team leading reliability through the asset life cycle, to indicate the effort at different life cycle stages.

For the case shown below, as the detail of the project increases, so too does the required reliability, integrity and risk management effort. Even at the earlier stages where effort may be lower, the reliability effort is still very important to ensure effective definition and delivery of the reliability and integrity requirements through the project stages.

Table A.1—TRC for Equipment

	Technical System Scale and Complexity			Operating Envelope	Organizational Capability
	Reliability	**Technology**	**Architecture/ Configuration**	**Environment**	**Organization**
Key-words	• Reliability requirements • Maintainability • Availability • Failure modes • Risk • Uncertainty	• Materials • Dimensions • Design life • Design concept • Strength 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, strains, and stresses • 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. Little or no relevant expertise. Limited resources/capacity to perform tasks.
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. Loss of relevant expertise. Loss of resources/capacity to perform work on multiple projects concurrently.
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:** In line with 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. Little or no loss of ability to perform functions. Collaboration and integration across activities.
D Low	**Acceptable 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 equivalent to previous specifications; interfaces remain unchanged, with no orientation or layout modification.	**Comparable environmental conditions:** Environment is comparable to recent project with no new environmental risks.	**Comparable team as previous:** Core project team, contractors, suppliers, and supplier's supply chain remain unchanged; applies throughout project life cycle. Well integrated and effective collaboration across team with demonstrated capability.

Table A.2—TRC for Procedures

	Technical System Scale and Complexity			Operating Envelope	Organizational Scale/Complexity
	Reliability	**Technology**	**Architecture/ Configuration**	**Environment**	**Organization**

Key-words	**General**
	• Procedure
	• Reliability Requirements
	• Failure modes
	• Verification/quality control
		General
		• Tooling
		• Materials
		• Measurement and control
		• Tooling qualification
		• Tooling calibration and certification
		Man & Assembly*
		• Product material
		Inst & Comm**
		• Diver/ROV
		Testing
		• Assembly design/function
		Intervention
		• Maintenance
		• Replacement
			General
			• Interfaces
			• Layout
			• Accessibility
			• Procedure reversibility
			• Dimensions
			Man & Assembly*
			• Interfaces
			  • Man-machine
			  • Machine-material
			  • Man-material
			• Assembled equipment
			Inst & Comm, Testing, and Intervention**
			• Interfaces
			  • Man-tooling
			  • Tooling-assembly
			  • Man-assembly
			• Integrated equipment
				General
				• Storage
				• Procedure loads
				• Procedural conditions
				Man & Assembly*
				• Manufacturing and treatment temperatures, pressures, and fluids
				Inst & Comm, Testing & Intervention**
				• Post-commissioning conditions
				• Field location
				• Water depth
				• Seabed conditions
				• Currents
				• Test temperatures, pressures, and fluids
					General
					• Location
					• Sub-suppliers
					• Personnel
					Inst & Comm, Testing & Intervention**
					• Roles and responsibilities

A Very high	**New reliability concept:** A significant reliability improvement requiring conceptual change to the procedure or tooling involved.	**Novel technology or new design (tooling/product/procedure) concepts:** Novel design or procedure to be qualified during project.	**Novel application:** Procedures (new or existing) have not been previously applied to these interfaces or geometries.	**New environment:** MATIC processes implemented under environmental conditions that are extended beyond previously applied levels such as temperature, pressure, or handling loads.	**Whole new team:** New team, working with new suppliers in a new location.
B High	**Major reliability improvements:** Major reliability improvement requiring change to the tooling or procedure.	**Major modifications:** Known designs (tooling/product) or procedures with major modifications.	**Major application modifications**: Major changes to procedure or interfaces/geometries to which procedures apply.	**Significant environmental changes**: Many changes to environmental conditions in which MATIC processes are undertaken, which 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 quality or procedural control.	**Minor modifications:** Same supplier using previously demonstrated tooling/procedures with minor modifications; modifications have been fully reviewed.	**Minor changes:** Minor changes to procedure or interfaces/geometries to which procedures apply. Changes reviewed and justified as minor.	**Similar environmental conditions:** Similar environmental conditions for MATIC processes as previous project or no major process operating envelope risks have been identified**.**	**Minor team changes:** Small or medium project organization; moderate complexity; minor changes in contractor/supplier and project team.
D Low	**Acceptable reliability:** No reliability improvements required and existing quality assurance (QA) and control is acceptable.	**Field proven technology:** Same supplier using previously demonstrated tooling/procedures; provide assurance no changes occurred.	**Unchanged:** Interfaces and geometries identical to previous applications; procedures remain unchanged, with no orientation or layout modification.	**Comparable environmental conditions:** Environment is comparable to recent project with no new environmental risks.	**Comparable team as previous:** Core project team, contractors, suppliers, and supplier's supply chain remain unchanged; applies throughout project life cycle with demonstrated capability.

*Man & Assembly—Manufacture and assembly.

**Inst & Comm—Installation and commissioning.

Table A.3—Example Level of Effort Expected for Different TRC Risk Levels Throughout the Asset Life Cycle

Technical Risk & Uncertainty	Feasibility	Concept Selection	FEED	Detailed Design	MATIC	Operation
A (Very high)	H	M	H	VH	VH	H
B (High)	H	M	H	H	H	M
C (Medium)	L	L	M	M	M	M
D (Low)	L	L	L	L	M	L

Annex B
(informative)

Detailed Description of Reliability and Integrity KPs

B.1 KPs for RIM

Oil and gas projects and operating assets require multiple organizations to work together to meet common objectives. For example, in addition to the installation contractor, there will be a number of contractors and suppliers who need to work with the operator, providing equipment and a range of services. While each of these organizations will have its own business objectives, when they come together in a project or work together to operate and maintain an asset, it is vitally important that there is a high degree of alignment of their processes and practices to enable the common objectives of the project or operation to be achieved efficiently.

Many operators, contractors, and suppliers will have organizational practices similar to those recommended in this RP. For example, most organizations have management systems that include MOC, project planning, and PRM. However, many of the other KPs may not be standard practice.

This document recommends that organizations collaborating in projects and in the operation of assets base their management around 12 KPs that support delivery of good RIM practice. The processes are generic and may be adapted by any of the collaborating organizations to align with their own internal management practices.

This section has been laid out to provide guidance on recommended activities for senior management as well as project and operations management to ensure the KPs are implemented successfully.

Four of these processes (Define Goals and Requirements; Planning and Organization; Design for and Deliver Reliability and Integrity; Feedback and Assurance) form the core DPIEF reliability and integrity assurance cycle that is applied throughout an asset's life cycle. The remaining 8 KPs provide support to the core processes (Figure 5).

B.2 Objectives and Preparation for All KPs

Operators are strongly encouraged to make reliability and integrity a core business value along with safety for all 12 KPs.

The objective is to ensure overall business and regulatory requirements provide the focus for delivery of reliability and integrity assurance. The objective for all of the KPs is to provide a management and process framework to ensure the delivery of high reliability and integrity throughout the asset life cycle. Key inputs to this are the need to:

— understand company policy and stakeholder requirements;

— understand statutory and regulatory requirements,

— define and agree the authority level for decision-making.

B.3 KP 1—Define Goals and Requirements

B.3.1 General

Defining goals and requirements ensures that the project and operational goals are fully aligned with overall business performance and regulatory objectives and provides the focus for delivery of reliability and integrity assurance.

B.3.2 Recommendations for Senior Management

— Define company and stakeholders goals and requirements. This will usually be the responsibility of the field operators in agreement with partners and stakeholders. The goals and requirements of engineering contractors and suppliers involved in projects or operations should be aligned with those of the field operator and any conflicts resolved.

— Define high-level objectives and set out the company's and stakeholders' policy and position on the achievement of reliability and integrity in projects and operations. Each organization within a project should define the authority level at which goals and requirements are specified, recommended, agreed, and approved.

B.3.3 Recommendations for Project and Operations Management

— Create a process with practical procedures and tools for defining project reliability and integrity goals and requirements.

— Implement agreed procedures for definition of reliability and integrity goals and requirements.

— Define project reliability goals and requirements that are consistent with company and stakeholders goals and objectives.

— Formally recognize the trade-off between the project engineering, hardware purchase capital expenditure (CAPEX), and the OPEX when:

  — defining reliability, maintainability, and integrity goals and requirements;

  — considering the need for reliability and maintainability improvement.

— Drive reliability and integrity goals and requirements to address the system architecture, equipment design requirements, and equipment qualification activities.

— Confirm that reliability and integrity goals and requirements are informed by and fully supported by the operations team.

— Confirm that project and operations management teams understand the difference between goals and requirements and how each will be managed.

  — Goals identify the reliability and integrity performance the project team would like to achieve. Goals are not mandatory.

  — Requirements identify the reliability and integrity performance that the asset is required to achieve in order to meet the business and regulatory objectives. These should be mandatory and included in acceptance criteria.

  — If management wish to ensure that nonmandatory reliability and integrity goals are given sufficient attention, reliability assurance should be mandated with a specific requirement to demonstrate the extent to which reliability goals have been achieved.

B.3.4 Process Description

B.3.4.1 General

Goals and requirements are statements that direct project and operations teams on what needs to be accomplished.

Selected goals and requirements should be specific and clearly defined, measurable, and realistically achievable within the specified time frame.

B.3.4.2 Specification of Reliability and Integrity Goals and Requirements

B.3.4.2.1 General

Organizations should consider reliability, availability, and integrity requirements in the following categories.

B.3.4.2.2 Management Related Goals and Requirements

- **KP Implementation.** Specify key RIM processes to be implemented within the scope of supply.
- **Management Capability Maturity.** Specify a capability maturity level to be achieved by a contractor or supplier (see KP 10 “Supply Chain Management”), particularly where the work is decentralized.
- **Analysis.** Specify a requirement to undertake specific analyses.
- **Design for X.** Specify a requirement to design for X, where X may include:
  - reliability (this is a process and may be included as a KP requirement);
  - maintainability (should include ability to isolate, retrieve, and replace);
  - ability to monitor equipment health, condition or failure status.

B.3.4.2.3 Qualitative Hardware Goals and Requirements

- **Reliability, Availability, and Integrity.** Some reliability, availability and integrity goals and requirements may be specified qualitatively. Typical examples are listed below.
  - Supplier is required to take appropriate actions to reduce the probability of failure from a specified failure mode.
  - Contractor is required to design hardware to be retrievable with a high level of accessibility when the reliability is low.
  - Supplier is required to implement manufacturing and assembly improvements to increase reliability and integrity.
  - An integrity requirement may be for no leakage of hydrocarbons to environment during the life of the installation.
  - A functional requirement for a subsea valve is to close on demand.

B.3.4.2.4 Quantitative Hardware Goals and Requirements

- **Reliability.** Specify a level of reliability required or desired for a component or a system.
- **Reliability Related to Equipment Performance.** It may be necessary to specify reliability related to performance. For example, it may be required for a pump to supply product above a specified rate.
- **Availability.** Specify a level of system or production availability to be achieved. When addressing “availability,” it is important to fully define the availability metric to be used. System availability may be specified for equipment items (e.g. SCM). Production availability may be specified for a complete installation.
- **Functional Performance Requirement.** A functional requirement for a subsea valve is to close on demand within a specified time.

— **Maintainability.** Specify a level of maintainability required for components, packages, or systems. This specification will normally take the form of a goal or requirement to achieve an MTTR and/or replace an item. This will also include the ability to isolate the item to facilitate retrieval for repair or replacement,

— **Maintenance-free Operating Period (MFOP).** Specify an MFOP. This is the period over which the equipment will not need to be retrieved for maintenance. It is a very direct metric and useful for driving reductions in early life failures of low reliability maintainable equipment. If the metric is to be used quantitatively, MFOP should be specified with probability P^*, the probability that the MFOP will not be achieved. If the component is assumed to belong to the exponential distribution, an equivalent required failure rate can be estimated using Equation (1):

$$\lambda = \frac{-\mathrm{Ln}\,(1-P^*)}{\mathrm{MFOP}} \tag{1}$$

Where P^* is the maximum allowable probability of exceeding the specified maintenance free operating period (MFOP) and λ is the failure rate of the item for which the MFOP is required.

NOTE This exponential distribution only applies to constant failure rates.

— **Failure-free Operating Period (FFOP).** Specify an FFOP (usually the FFOP would not be less than the life of the equipment). This is the period for which the equipment is required to operate without failure and is useful for equipment that cannot be maintained or is very difficult or expensive to repair such as wellheads, pipelines, flowlines, etc. If the metric is to be used quantitatively, then FFOP should be specified along with an acceptable probability P^*. The failure distribution for components that are required to be failure free for life do not normally follow the exponential distribution.

— **Integrity.** Specify an acceptable probability of loss of containment. This will normally depend on failure consequences (e.g. size of the leak). For safety critical equipment, this may be specified as a probability of failure on demand or an SIL.

  — An example of a performance requirement for a subsea seal might take the form “subsea seal must withstand a pressure of 5000 psi.” An associated reliability/integrity requirement for this example might be “subsea seal must withstand a pressure of 5000 psi with a probability of intervention for replacement of less than 2 % over the defined life of 25 years.”

— **Integrity Related to Equipment Performance.** It may be necessary to specify integrity related to performance. For example, it may be necessary for a valve to close within a specified time.

B.3.4.2.5 Guidance on Quantitative Goals vs Quantitative Requirements

— Where an installation has to produce a guaranteed output through an agreed contract (e.g. gas production contract), production availability may be defined as a requirement.

— Where the installation output has no contractual constraints, reliability and availability metrics should be specified as goals.

B.3.4.3 Allocation of Goals and Requirements

Reliability and integrity goals and requirements are generally defined at a high level early in the project life cycle. For example, a new subsea field development may have been set a production availability goal. As the project progresses, the high-level goals need to be allocated down to package level such that by the end of the FEED stage, reliability, availability, and integrity goals and requirements can be specified for the main equipment packages.

The process of reliability and integrity allocation down to package level should be considered for all high-level goals and requirements, both qualitative and quantitative.

The procedure outlined in B.3.4.5 may be used to define reliability or integrity requirements.

Where qualitative requirements have been set, the process of allocation can be undertaken by sequentially asking how the goal or requirement is to be achieved. This “what/how” questioning continues until a practical action has been defined.

In many cases the allocation process will lead to a requirement to perform other analyses to further understand what actions to take. For example, suppose the high-level goal is “to reduce early life failures.” On questioning how this is to be achieved, one action might be to perform a review of failures experienced by the operator, either through a lessons learned review or through data analysis. This analysis might then lead to recognition of potential risks to reliability achievement. Once these risks are identified, actions can be defined to prevent or at least reduce the likelihood of occurrence.

B.3.4.4 Strategy for Achievement of Reliability and Integrity Goals and Requirements

Projects and operations should develop a well-defined strategy for achieving the specified reliability, availability, or integrity goals or requirements during field development and field operation.

Example strategic considerations include the following.

— **Qualification Strategy.** Use of field proven equipment rather than new technology.

— **Standardization Strategy.** Use of equipment conforming to company or industry standards.

— **Reliability Strategy.** May be required when the maintenance cost is very high. A reliability strategy should consider the introduction of design for reliability, redundancy, additional qualification effort, and/or greater QC in manufacture.

— **Maintenance Strategy.** Achievement of availability through rapid maintenance intervention and light well intervention vessel strategy.

— **Maintainability Strategy.** Achieve a required level of production or system availability by minimizing the time to restore failed equipment to an operable state. A maintainability strategy should consider low reliability items, spare part inventories and the ease of keeping or restoring the system to an operational state.

— **Risk Mitigation Strategy.** Use operational mitigations, such as spare capacity, to reduce the effect of system failure.

— **Integrity Strategy.** Design redundancy into the system to ensure integrity is maintained.

— **Production Availability Strategy.** Achieve a required level of production to ensure business objective is maintained.

— **Obsolescence Strategy.** Identify equipment that are likely to become obsolete within the life cycle of the asset and develop an obsolescence management plan.

B.3.4.5 Procedure for Allocation of Goals and Requirements

The definition of goals and requirements for inclusion in a supplier 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. The steps involved in the allocation process are outlined below.

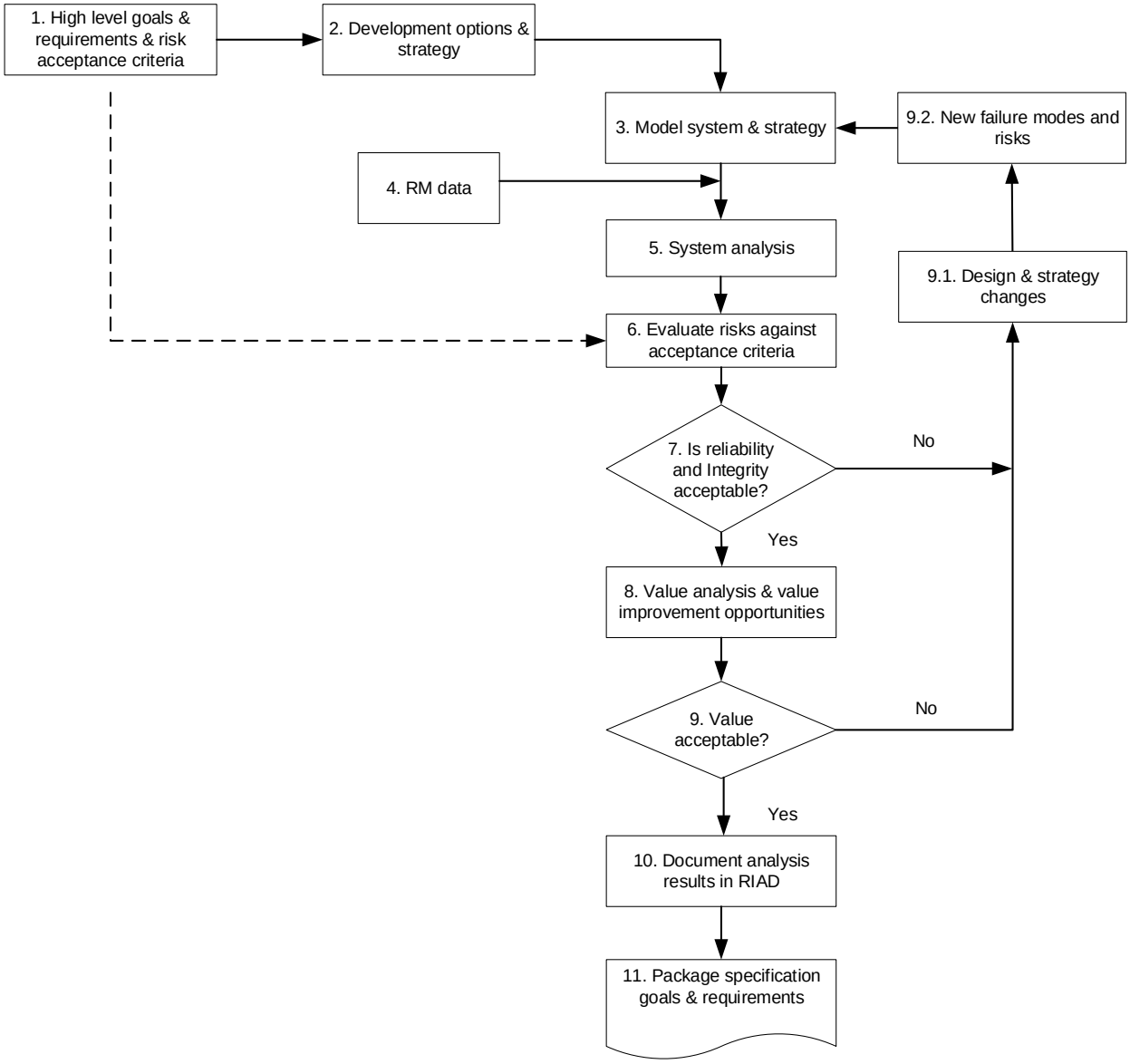


Figure B.1—Procedure for Allocation of RIM Goals and Requirements

Step 1. High-level Goals and Requirements

Define high-level goals and requirements to align with overall business objective for the asset. High-level goals and requirements can cover a whole range of issues including:

— production requirements, i.e. the ability to maintain uptime and minimize downtime;

— integrity requirements, i.e. the ability to isolate and contain;

— reliability, availability, and integrity acceptance criteria can be based on the defined goals and requirements.

Step 2. Development Options and Strategy

Identify feasible options for the field development and define the focus of the strategy, capable of delivering the high-level goals and requirements (see B.3.4.4). This RP recommends implementing a reliability,

integrity, and technical risk management program that has the ability to combine some, or all, of the strategies listed in B.3.4.4.

Step 3. Model System and Strategy

Create a model that represents the system reliability and integrity logic and the strategy. Reference should be made to KP 5 (reliability, availability, and integrity analysis) to identify suitable techniques for representing the system and strategy.

- Typical system modeling tools include:
  - RAM analysis for production and system availability;
  - reliability block diagram (RBD) analysis for system reliability analysis;
  - fault tree analysis (FTA) or event tree analysis (ETA) for integrity analysis.
- System models 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.
- The selected concept should be further detailed in FEED.

Step 4. RM Data Input

Input valid historical data where practicable.

- Generic data with constant failure rates for components are available through databases such as offshore reliability data (OREDA) or pipeline and riser loss of containment (PARLOC) study.
- Field-specific data may be obtained through operator's own database.
- Where specific data are not available, analyses may be required to estimate reliability or integrity.
- 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).
- Sensitivity studies should be undertaken to reflect uncertainty in the data.

Step 5. System Analysis

Perform the required reliability, availability, or integrity analysis.

Step 6. Evaluate Reliability, Availability, and Integrity Against Acceptance Criteria

- Evaluate the assessed system result (its reliability, availability, or integrity) against the acceptance criteria specified in Step 1.
- At concept selection stage, the evaluation against the acceptance criteria should be used to support the decision regarding which concept is to be developed 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).

Step 7. Acceptance Decision

— If the assessed reliability or integrity is below the specified goal or requirement, then design actions should be taken to improve performance (see Step 9).

— If the assessed reliability or integrity is greater than or equal to the specified goal or requirement, then consideration should be given to the value of further improvements.

— Compare the output from the RAM analyses with availability goals and requirements (acceptance criteria). If the design and item RM data satisfy 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.

Step 8. Value Analysis and Value Improvement Opportunities

Reliability value (cost-benefit) analysis is used 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, integrity, maintainability, and intervention logistics.

The reliability of hardware packages has significant impact on operational expenditure. Package reliability and integrity improvement may decrease OPEX, decrease deferred production losses, and hence increase field value. However there may be increased CAPEX associated with realizing reliability and integrity improvements.

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

Quantitative reliability and integrity 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 and integrity 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 and integrity value analysis may require economic simplifications. Consequently, reliability and integrity value analysis should not be considered as a method of full economic appraisal and should only be used as a method of comparative analysis.

Step 9. Value Acceptable

As a method for comparing design options, a reliability and integrity based decision criteria may be formulated. The sensitivity of the system and system elements to the value metric should be assessed and reviewed to ascertain the scope for value improvements.

Step 9.1. Design and Strategy Changes

Many changes to design or strategy are related to technical (reliability and integrity) or flow assurance considerations. 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 input data.

If the system layout has been finalized but the predicted performance does not meet the acceptance criteria, then individual items may require reliability and integrity 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.

Step 9.2. New Failure Modes and Risks

New failure modes are identified and described. Potential failure modes are determined by examination of item outputs and functional outputs identified in applicable block diagrams and schematics. Failure modes of the individual item function are based on the stated requirements. The new risk items may warrant special attention in design and manufacture due to their criticality to project success. A list of priorities should be prepared to highlight those hardware items that represent significant risk to a project.

Step 10. Document Analysis Results in RIAD

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.

Step 11. Package Specification, 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 senior management.

B.4 KP 2—Planning and Organization

B.4.1 Objectives and Preparation for KP 2

The planning and organization process allocates leadership and resources to the required RIM activities such that they add value to the asset overall and do not adversely impact on schedule requirements.

The planning and organization process ensures that the project and operational goals are fully aligned with overall business performance and regulatory objectives and provides the focus for delivery of reliability and integrity assurance.

B.4.2 Recommendation for Senior Management

Create a process for planning and organizing for RIM, as follows.

- Create high-level process documentation to address planning and organizing for RIM in project and operations phases. This should refer to:
  - high-level policy documentation outlining company expectations for meeting company and regulatory goals and requirements;
  - management expectations and procedures for handling emergent risks in the project as described under KP 7.
- Demonstrate commitment to delivery of systems reliability and integrity through:
  - provision of sufficient resources to manage the scope, scale, and complexity of projects and operations;
  - provision of sufficient flexibility in time and manpower resources to manage emergent reliability and integrity issues as the project progresses through its life cycle.

— Provide training that ensures that the project management team has complete understanding of the need for and commitment to delivery of reliability and integrity. This should include guidance on the types of reliability activities that may be needed and the level of resourcing that may entail.

— Define and agree the authority level for project managers to resolve conflicts between project budget and schedule deliverables and meeting reliability and integrity goals and requirements.

B.4.3 Recommendations for Project and Operations Management

— Create plans for delivery of reliability and integrity that are consistent with company objectives and that address:

  — work scope;

  — timing and duration;

  — engagement with related project engineering activities;

  — quality of deliverables;

  — management of actions arising from reliability and integrity activities;

  — verification and validation of planned activities.

— Work with senior managers to agree budgets and timescales that are realistic and achievable for meeting reliability and integrity goals and requirements.

— Ensure that all emergent risks to project success are identified, assessed, managed, and communicated to senior management.

— Ensure that risk and reliability activities are undertaken at the right time with the right tools and competent reliability engineering resources.

— Ensure that all planned activities have a clearly defined specification, i.e. clear objectives and requirements that have to be met.

B.4.4 Process Description

B.4.4.1 General

Planning and organization for reliability and integrity should be implemented at each project life cycle stage regardless of the project technical risk (TRC) and on a regular basis (e.g. annually) through operations.

The purpose of the planning and organizing process is to:

— develop and maintain a plan for implementing the required reliability and integrity scope of work to support achievement of reliability and integrity goals and requirements and management of identified technical risks;

— identify key roles and responsibilities for management and delivery of reliability and integrity.

The level of resourcing and effort required should be related to the level of technical risk associated with the achievement of the goals and requirements. This RP recommends the use of TRC (see Annex A).

B.4.4.2 Planning

Reliability and integrity planning starts at the feasibility stage of a project. The plan should be regularly updated through all project stages over the whole life cycle of the field development and throughout operations.

Early in the project life cycle, a simple table identifying each activity in the scope of work may suffice. A more substantial plan is expected during FEED and subsequent life cycle stages with equipment suppliers and installation contractors preparing plans for their scope of supply.

The reliability and integrity activities identified should be considered an integral part of the engineering process and integrated with conventional engineering tasks in the project management system. The reliability and integrity plan should be integrated with the wider project delivery and operational readiness plans to ensure that all elements of the project remain coordinated and that the implications of any RIM activities are addressed.

The required reliability and integrity scope of work should be broken down into specific activities and associated tasks. The plan should identify:

— required activities (e.g. analyses, tests) and associated tasks (e.g. collation of input data for RAM analysis);

— specific resources required to implement each activity (e.g. facilities, key expertise, personnel) and, if required, associated resource costs;

— deliverables from each activity;

— associated verification and validation tasks;

— the appropriate schedule and milestones for the activities recognizing the wider project schedule demands and the need for output to interface with decision-making;

— responsibilities for:

  — implementing each activity;

  — overall delivery of reliability and integrity.

In addition, it is useful to include the following information in the plan to support identification of appropriate activities and an appropriate level of resourcing:

— the relevant TRC (or alternative novelty/risk assessment);

— goals and requirements.

The TRC should be used to focus attention on equipment/procedures of high technical risk and direct the appropriate analysis techniques to the sources of technical risk (see the change risk factors in Table A.1—Table A.2 and in Annex A.3 for more guidance).

Table A.3 provides an example of the relative level of effort anticipated for each technical risk category at each life cycle stage. As the level of detail increases and the risk category increases so the planned effort for each task should increase in relation to both:

— the time to completion;

— a shift toward increasingly more quantitative activities (see Figure B.2).

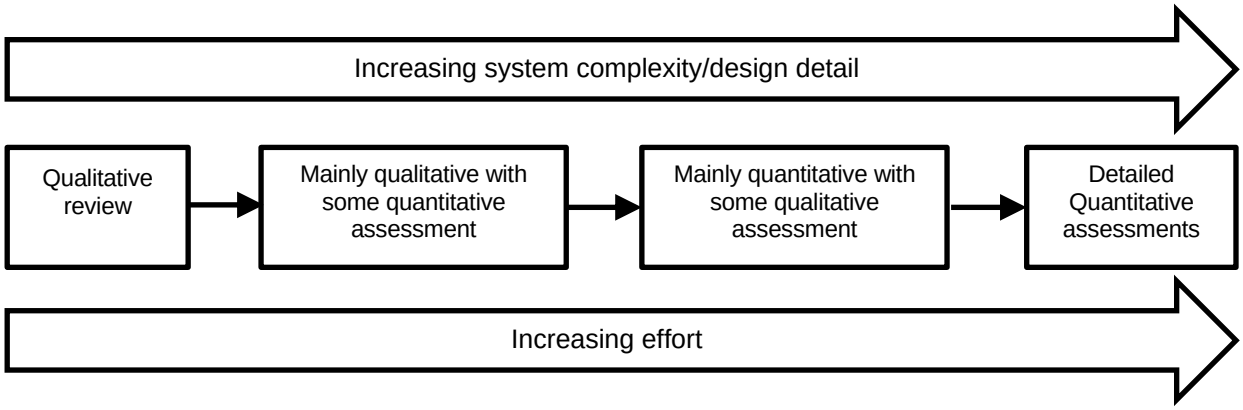


Figure B.2—Reliability and Integrity Activity Effort

When resourcing activities it is recommended that:

— installation contractors are included in design reviews during FEED or detail design;

— operations and maintenance knowledge is utilized throughout the design process to ensure the design takes account of lessons learned by end users and operators.

Once the appropriate level of effort and resources for each task have been defined, the plan can be formulated with the aid of conventional project management tools and practices.

When scheduling reliability and integrity activities for the MATIC stages and early life operations, many activities should be implemented during earlier life cycle stages (e.g. Installation plans and risk assessments are performed in advance of the installation stage).

During each life cycle stage, updates may be needed to the plan to reflect:

— changes to the design or an associated procedure;

— updates to the risk categorization of the system, a package, component, or procedure;

— requirements for additional activities to be performed or unnecessary activities deleted.

B.4.4.3 Organizing

There are various approaches that may be adopted in organizing for delivery of reliability and integrity. This will depend, amongst other things, on the size and scale of the project and the operator preferences.

Responsibility for ensuring reliability and integrity achievement will vary and depend on company policy. Typically, at the project stage it will reside with senior managers responsible for ensuring the delivery of the subsea system to time and budget. However, operational experience is a key input to decision-making to ensure that the strategy adopted by the design and development team will deliver acceptable levels of production reliability and integrity performance. The operations team should play a significant role in monitoring and advising the project team during the project stage.

Analytical tasks and coordination of reliability and integrity activities may be outsourced to reliability and integrity specialists if there are insufficient internal resources and expertise. However, it is crucially important that:

— reliability and integrity activities are fully integrated with engineering activities;

— analytical tasks and operational inputs inform design decision-making;

— reliability and integrity decisions are followed up, acted on, and closed out in a timely manner;

— there is effective teamwork between reliability engineers, package engineers, system integration engineers, reservoir engineers, and appropriate technical specialists.

It is helpful to assign ownership to each of the reliability and integrity activities and to delegate responsibility for the implementation of the reliability and integrity activities and associated tasks.

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 and integrity responsibility and activity ownership at the various levels of technology indenture. The capability of each organization should be addressed for this situation (see B.12.4.2).

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

— **Project Reliability and Integrity Champion or Technical Authority.** The reliability and integrity champion or technical authority should ideally be a senior engineer or advisor with authority and influence. The champion would not normally be the person in control of the project but should have a strong influence. The role would essentially be that of advocate and high-level reliability problem solver.

— **Project Reliability and Integrity Delivery Manager.** The reliability and integrity delivery manager should be the subsea system delivery manager, or project manager, in charge of the overall project. He/she will be responsible for ensuring that adequate resources are available to meet reliability, cost, and schedule requirements.

— **Project Package Engineer.** Responsibility for meeting cost and schedule requirements for package reliability and integrity activities may be delegated to package lead engineers. They would be responsible for managing the reliability and integrity activities in their area of responsibility but not necessarily performing them.

— **Project Reliability Engineers.** Specialist reliability and integrity engineers may be employed to support projects. The reliability specialist should have specialized 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 risk analyses (e.g. FMECA) and modeling (system reliability/availability models).

— **Project Reliability and Integrity Assurance Engineer.** A separate reliability and integrity assurance engineer may be appointed to take responsibility for managing the collation and integration of all relevant project availability outputs and its compilation into the RIADs.

— **Operational Reliability and Integrity Engineer.** This role should be performed by an experienced reliability and integrity engineer reporting to, and with direct support from, the installation managers. The reliability and integrity engineer should be experienced in RCA and be responsible for data management and analysis.

— **Verification and Validation Authority.** Verification and validation activities may be allocated to a specialist engineer or technical authority. This may involve internal staff or may involve independent external consultants.

B.5 KP 3—Design for and Deliver Reliability and Integrity

B.5.1 Objectives and Preparation for KP 3

Design for and deliver reliability and integrity (DfRI) is the KP for developing and delivering reliability and integrity of subsea installations. It addresses all the design life cycle stages together with the MATIC and operation stages.

Its primary aim is to design-in features at component or overall system level that will prevent or reduce the likelihood of failure or degradation in operation by using appropriate reliability engineering analysis and testing techniques, applied at the right time, to inform design decisions.

As far as practicable, components and equipment packages should be designed to an acceptable level of reliability by the supplier outside of a field development project, as part of the suppliers DfRI strategy before procurement. DfRI continues into projects, with the design of the subsea system architecture to meet reliability and integrity requirements.

— Senior management within the operator's organization should develop guidance for project engineering staff and contractors on procedures and practices to be followed in designing for reliability and integrity in field development projects.

— Senior management in the OEM/supplier should define expectations and provide resources to develop:

  — DfRI strategy and processes to deliver high reliability and integrity performance in their equipment;

  — Relevant guidance for application in the development process.

B.5.2 Recommendation for Product Development, Project Management, and Operators

— Operators should develop equipment procurement procedures that include reliability and integrity in the equipment specification to drive the supplier's DfRI process including quality assurance and control in the MATIC stages.

— Product development managers within the supplier organization should ensure that equipment within their scope of supply are designed to be robust and achieve or exceed the reliability and integrity requirements specified by the customer, or make clear what is realistically obtainable so that project targets are realistic.

— Field development project managers should ensure that the system architecture and procured equipment are designed and then delivered though the MATIC stage to achieve reliability and integrity requirements within project constraints.

— Field operators should apply the processes in this RP to ensure that the designed-in reliability and integrity continues to be delivered during operations.

B.5.3 Process Description

B.5.3.1 General

DfRI is a continuous process that starts in the OEM's organization and continues into the operator's project organization, throughout the whole project life cycle.

DfRI is considered an extension of good engineering practice but requires increased focus on understanding how and why failures occur in operation. Consequently, actions taken during product development or during projects to achieve reliability and integrity goals and requirements should be based on the best possible information and data gathered through timely reliability and integrity assessment studies. For example, systems reliability and value analysis may help the project or development team to decide on the approach

to reliability improvement when the system has unacceptable reliability performance (e.g. whether to adopt a redundancy strategy or whether to select a more reliable component).

The DfRI process can be applied at any level of the design from parts and components through to whole systems and a complete field and is comprised of three fundamental activities integrated into the design process as shown in Figure B.3.

— **Analyze Design.** Perform reliability and integrity analyses on the proposed design.

— **Evaluate Design.** Evaluate the results against reliability and integrity goals and requirements.

— **Improve Design.** Improve the design to meet or exceed customer, company, or regulatory reliability and integrity requirements.

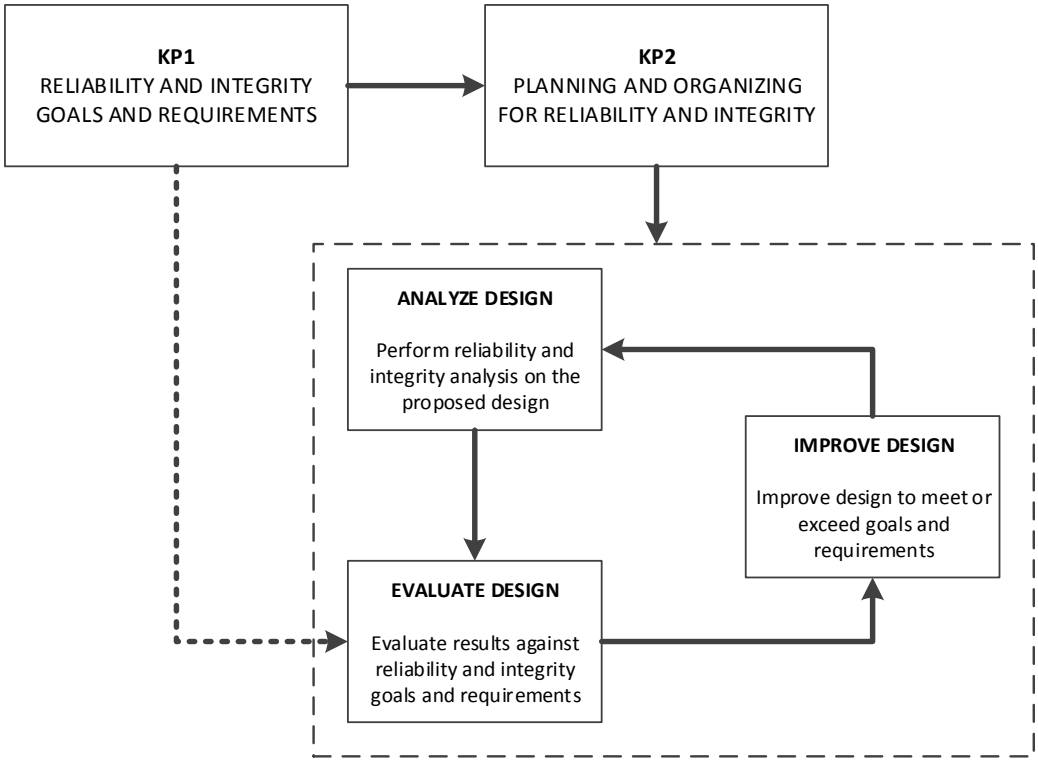


Figure B.3—Design for Reliability and Integrity Process

B.5.3.2 Analyze Design

The first step in implementing a DfRI program is to understand what improvements need to be made and where they need to be made. This is accomplished by performing analyses and where necessary tests as defined in KP 2 to assess the reliability and integrity performance and deliver qualified equipment to the project; this should apply to all design concepts.

Useful input studies for DfRI typically include but are not restricted to:

— TRC;

— technology readiness assessments;

— reliability and integrity allocations from defined goals and requirements;

— systems reliability and integrity analyses and models;

— qualification testing of equipment;

— system or component reliability value analyses.

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.

The defined RIM strategy will impact on decisions. For example, the design team may need to focus on reliability, integrity, or maintainability or a combination of all as the means of achieving an availability goal. Clarity will be needed in order to prioritize design decisions.

The intent of these studies is to enable the product development team or the project team to see what improvements need to be made and where they need to be made.

B.5.3.3 Evaluate Design

The second step of the DfRI strategy is the evaluation of the assessed reliability and integrity performance against the specified goals and requirements. This is a key decision that could have major financial impacts both on the customer and on the supplier, depending on the outcome.

There are likely to be important trade-offs between project risks (schedule and budgets) and operational risks. It is important therefore to ensure that there is a defined and agreed authority in making this decision and that all relevant stakeholders are involved and informed of outcomes in sufficient time to take appropriate actions.

B.5.3.4 Improve Design

A reliability-focused design requires particular attention to be paid to understanding failure modes, failure mechanisms, and root causes of failure. Reliability and integrity improvements cannot be achieved without this knowledge.

B.5.4 Additional Guidance

B.5.4.1 Supplier Responsibilities

The suppliers design intent in DfRI should be to design and develop a robust design that is insensitive to variation in the operating environment to which it may be exposed. It should be tolerant of faults or damage and continue to function to an acceptable level of performance without loss of containment or production capability. This should ideally be undertaken outside of a project.

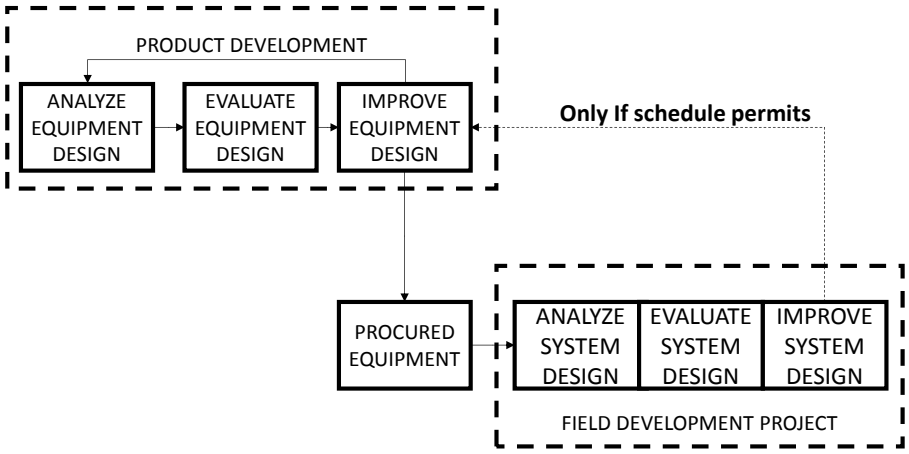


Figure B.4—Relationship Between Operator's DfRI and Supplier's DfRI Processes

B.5.4.2 Preventing Failures During Design Stage

There are many ways that a component design or a system design may be made robust and reliable. There may be trade-offs between some options (e.g. redundancy vs the desire to simplify a system, or integrated vs modular design) that should be considered. Some examples of considerations are listed below.

- Eliminate known failure modes through technology change.
- Reduce the probability of failure mode occurrence by:
  - eliminating failure mechanisms/causes through design change;
  - preventing failure mechanisms/causes through effective QC/QA;
  - reducing the probability of human error triggers to failure causes.
- Reduce complexity through:
  - system simplification;
  - parts count reduction;
  - reduction of interactions between different systems/components.
- Reduce internal loads, stress and fatigue, and where possible, external loads:
  - Static;
  - dynamic/cyclic;
  - shock.
- Increase strength.
- Select materials, fabrication processes, and weld designs with low susceptibility to degradation mechanisms:
  - hydrogen-induced stress corrosion cracking (HISC);
  - chloride stress corrosion cracking (SCC);
  - pitting and other forms of localized corrosion.
- Consider compatibility of materials and the adverse effects of galvanic corrosion.
- Consider use of corrosion resistant materials for coatings.
- Improve interface reliability.
- Introduce redundancy.
- Reduce common cause failures or reduce their probability of occurrence.

Provide sensors and monitoring systems. 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 maintainability considerations include:

- improve system inspection capability;
- online monitoring of equipment condition and status;
- “hot” tapping and intervention for repair;

— improve interface accessibility;

— design for ease of replacement of unreliable components;

— reduce interface complexity;

— availability of spares;

— design in the ability to run in-line inspection (ILI) and cleaning pigs in operation.

System availability simulation (e.g. RAM analysis) tools will be useful in supporting design decisions aimed at assessment of the maintenance strategy and reducing system downtime.

B.5.4.3 Preventing Failures During MATIC Stage

B.5.4.4.1 General

A significant proportion of subsea failures, especially those occurring in early life, arise as a result of faults or defects introduced post design (e.g. during MATIC) in an otherwise reliable product. Many of these delivery faults arise as a result of human error or technical failures occurring in the manufacturing or installation processes.

The DfRI strategy should address the risk of damage to equipment and failures occurring during the MATIC stages. A robust design requirements strategy is an important means to account for cross-functional and cross-life-cycle input to the design:

— enabling QC in manufacture;

— enabling verification during installation and commissioning.

B.5.4.4.2 Robust Design Strategy

Equipment may experience loads/stresses and environments during transport and installation that are completely different from that expected in operation.

Robust design principles described above may be applied to address the MATIC stage. Particular attention should be paid to:

— static, dynamic, and shock loads during transport and installation;

— preservation of equipment e.g. unexpected exposure to seawater in the event that equipment has to be wet parked.

Where the technology is new or existing technology is to be used in a new environment, the technology qualification program (TQP) should address reliability and integrity requirements for MATIC as well as operation stages. For example, the OEM may consider the use of highly accelerated life testing (HALT) for electronic equipment to support creation of a robust design during product development and equipment qualification.

B.5.4.4.3 Enabling QC in Manufacture

Equipment reliability during system operation may be improved by preventing faults and defects being introduced during manufacture. This may be achieved by close attention to QC requirements during the design process.

B.5.4.4.4 Enabling Verification During Installation and Commissioning

Particular attention to installation and commissioning requirements, procedures, etc. should be accounted for in design. Verification of product/system design features that affect functional reliability and integrity should be included and accounted for in the design phase.

B.6 KP 4—Feedback and Assurance

B.6.1 Objectives and Preparation for KP 4

Feedback and assurance is the process of communicating information pertaining to reliability, integrity, and technical effectiveness of the system to members of a project/operations team and to senior management.

B.6.2 Recommendation for Senior Management

Senior management in the operator's organization should develop expectations for internal policies relating to reliability and integrity assurance and ensure that there is a process in place with procedures for:

— capturing, storing, and retrieving lessons learned in projects and operations;

— reporting failures and corrective actions (e.g. FRACAS);

— providing assurance that the project teams and equipment suppliers are delivering equipment and systems that meet defined reliability and integrity goals and requirements;

— creating documented reliability and integrity assurance evidence;

— ensuring compliance with regulatory requirements.

B.6.3 Recommendations for Project and Operations Management

Project managers should ensure that:

— projects benefit from previous lessons learned through retrieval of lessons learned documents or workshop activities;

— projects capture and store lessons learned in each project stage;

— lessons learned procedures are in conformance with company defined policy and procedures;

— RIADs are created and communicated to senior managers.

Operations managers should ensure that:

— lessons learned from operations are captured and communicated to central engineering groups, senior managers, and to future projects;

— effective measures are in place for acquisition and assessment of field data and for its communication within the company;

— FRACAS has been developed and made available for operations use.

B.6.4 Process Description

B.6.4.1 General

The following three activities should be included within the reliability and integrity assurance process:

— feedback of lessons learned;

— operator's TRARs where appropriate;

— preparation and issue of RIAD.

B.6.4.2 Feedback of Lessons Learned

Lessons can be learned from all phases in the life cycle of an installation from feasibility through the project life cycle into operation. Feedback of information from projects and operations should be captured to support future learning.

A review of the reliability engineering and integrity management activities both in projects and operations should be undertaken to provide feedback and learning related to the effectiveness of processes and implementation of procedures.

A lessons learned and best practice register should be created early in the project life cycle and updated at the end of each project stage and on an ongoing basis during operations. Captured lessons and best practice should be transferred to a central knowledge management system for use by future projects and other operating assets.

Feedback of lessons learned from operations is particularly valuable and strongly recommended. Knowledge of lessons learned from operating assets enables project teams and future operations teams to deliver improved performance.

Performance data for the asset obtained from testing/analysis prior to deployment and subsequently from integrity management activities in operations should be collected and analyzed to:

— identify corrective actions and improvements;

— confirm asset integrity and availability performance;

— validate project reliability and integrity performance predictions;

— identify any required revisions to the integrity management system for the asset;

— provide reliability data for the operating asset;

— support future project reliability and integrity analyses;

— provide data for input to reliability databases for use by future projects;

— provide feedback to suppliers on equipment reliability and integrity performance;

— enable reporting to legislative authorities, management, and third parties.

Operators are recommended to develop FRACAS as a core element of the reliability and integrity assurance process.

B.6.4.3 Operator's TRAR

For equipment that is categorized as high technical risk, i.e. TRC A or B, the operator should undertake a review of the risks relating to supplier's equipment to obtain assurances that the equipment will meet reliability and integrity goals and requirements. System-level reviews are recommended toward the end of FEED and component reviews in detailed design ahead of manufacture.

The purpose of the TRAR is to identify problems and gaps in the reliability, integrity, and technical risk management program, for example to identify residual risks and failure modes that may compromise reliability and integrity of suppliers equipment in operation or during transport installation or commissioning.

The TRAR should include but may not be limited to the following considerations:

- equipment design:
  - design standards used;
  - current status of the design;
- equipment functions (primary, secondary, etc.) and performance:
  - required;
  - achieved;
- seals and containment assurance:
  - seal design used;
  - tests undertaken and planned;
- reliability and integrity goals and requirements:
  - current status (reliability assessments);
- review of FMECA studies performed:
  - main risks identified;
  - risk management actions taken;
- materials and compatibility,
  - bulk materials;
  - chemicals and fluids;
  - coatings;
- expected loads and stresses and actions taken to manage,
  - in operation;
  - in MATIC;

- expected environments and actions taken to manage:
  - in operation;
  - in MATIC;
  - during storage;
  - during transit;
- current TRL:
  - existing evidence;
- qualification testing to meet required TRL:
  - testing undertaken;
  - planned testing;
- product and service conformity:
  - nonconformance trends;
  - field failure analysis;
- status of corrective and preventive actions;
- risks related to the supply chain:
  - bought-in items;
  - manufacturing requirements;
  - supplier/sub-supplier activities;
  - supplier/sub-supplier performance.

The output of the TRAR is a report that should include the following:

- summary of issues addressed;
- list of action items to close gaps in supplier's risk assessments and to manage the residual risks.

B.6.4.4 RIAD

Reliability and integrity assurance is the process of collating/assessing equipment and processes to provide evidence of integrity and availability achievement and communicating this information in a formal document.

Reliability and integrity 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.

This information is generated during a project and updated during operations so that the end customer has the best possible indication at any stage during the asset life cycle of the system's current and eventual

technical effectiveness. Technical effectiveness includes a system's functional performance attribute (which includes integrity) and a system availability attribute (which includes reliability, durability, and maintainability).

The key output from the reliability and integrity assurance process is the RIAD. The purpose of the RIAD is to provide the stakeholders with evidence of progressive achievement during the project and operations.

The RIAD is a living document initiated at the feasibility stage of a project and continually updated throughout the asset life cycle stages.

B.6.5 Additional Guidance

B.6.5.1 Reliability and Integrity Assurance Evidence

Documented evidence provided in the RIAD will vary in quality depending on its source. Table B.1 provides comments on the different data types available.

Table B.1—Types of Reliability and Integrity Assurance Evidence

Evidence Type	Comment
Current Field Data	These are the most representative 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 unreliable or incomplete].
Test/Trial Data	Trial data can more closely replicate actual conditions in comparison to previous use data for equipment that has been modified.
Expert Opinion	May be appropriate in cases where the technical expert is a recognized authority or subject matter expert.
Previous Use Data	These are possibly the most abundant data, especially for mature technology. However, close attention should be directed toward 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.
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.

B.6.5.2 RIAD

The size of the RIAD should reflect the sources and levels of project and technical uncertainty and/or risk and the level of assurance detail required by the operator or user of the equipment. It may be a simple document referencing other documents containing, for example, the system requirements and the assurance evidence.

In practice an RIAD may comprise, or reference, a number of documents from a variety of sources to capture the information indicated in Table B.2, which may be used as a guide to the construction of an RIAD.

The RIAD should be tailored to reflect the required assurance and decision support at the different life cycle stages. There may be two basic types of RIAD created during a project: a system or project RIAD and a more detailed equipment RIAD.

The system or project RIAD may include a high-level synopsis that is included as part of the decision support package for the project stage gatekeeper to support decision-making (e.g. continuation to the next project stage or selection of preferred concepts).

Equipment RIADs may be more detailed to support the claims of the integrity and availability performance; where appropriate, they should also reflect the accumulated assurance and continuous improvement of equipment over multiple asset application throughout the equipment's life cycle. The RIAD, therefore, becomes a living document both over the course of an asset life cycle but also an equipment's life cycle.

Table B.2—Suggested Constituent Parts of an RIAD

System Description	A clear definition of the operating environment and system layout should be included and may be referenced as an external document.
Integrity and Availability Requirements	Include the integrity and availability goals and requirements defined for the equipment. Include any process or procedural requirements.
Integrity and Availability Baseline Condition	The method of measurement and outcome of an established baseline against which future integrity and availability can be measured.
Strategy for Integrity and Availability Achievement	Summarize the strategy implemented to achieve the project and asset goals and requirements, including an indication of the technical risk as defined by the TRC with justification of the category selected and an indication of the level of effort required.
Reliability and Integrity Plan	The plan of reliability and integrity tasks defined to deliver the integrity and availability performance can be fed directly into (or referred in) the assurance document.
Integrity and Availability Evidence	Present the summarized results of any reliability and integrity activities implemented as part of the project and during operations. 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.1 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.
Key Assumptions	Present any key assumptions made during analysis, modeling, testing, or used in any subsequent integrity and availability claims. During operations key assumptions should be checked and validated.
Integrity and Availability Claims	Any claims of the technical effectiveness made on the basis of the integrity and availability evidence should be included.
Limitations on Use	Some activities will have determined the operational envelope or operational conditions that prevent the confident delivery of the integrity and 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 and integrity activities are specified here.
References	References to external documents.
Appendices	Include the bulk of the data generated during the project and through operations that is not referenced externally.

B.7 KP 5—Risk and Availability Analysis

B.7.1 Objectives and Preparation for KP 5

Risk and availability analysis supports the identification and evaluation of failure modes and their associated risks (consequences and the frequency of occurrence). Its primary aims are to understand the underlying causes of failure, the inter-dependencies in a system, and actions to manage risk to achievement of asset goals and requirements. The risk may be quantified in terms of safety, environment, production availability, or financial.

B.7.2 Recommendation for Senior Management

— Define expectations for processes for the management of reliability, availability, and integrity analysis in projects and operations. This should address provision of:

  — technical specialists to advise on the need for analysis and the type of analysis that may be required by a project or operations;

  — analysis and modeling tools and techniques to be used by project or operations team;

  — templates for analysis or reporting of analyses;

  — internal or external specialists in the use of the tools and techniques.

— Define expectations and provide resources for the creation of guidance documents, integrated with company policy and execution processes, which describe:

  — tools and techniques to be used and their integration into the design process;

  — reasons for using a specific tool or technique;

  — limitations/boundaries of use;

  — how and where to access tools and templates.

— Provide access to relevant training for project and operations teams in the practical use of tools and techniques and their associated integration into design execution processes.

B.7.3 Recommendations for Project and Operations Management

— Ensure that tools and resources are readily available for projects and operations to address technical risk, component reliability, system reliability, system or production availability, and system integrity.

— Implement tools at the right time and with the right level of effort to ensure that analysis work keeps pace with the project.

B.7.4 Process Description

B.7.4.1 General

Risk and availability analysis processes are required to support projects and operations in understanding how systems, components and processes function and how they can fail.

The output from the analyses enables clear prioritization of required activities and actions to minimize risk and optimize reliability/availability.

B.7.4.2 Purpose and Goal of Analyses

Analysis should be focused on demonstrating the extent to which reliability and integrity goals and requirements are likely to be met. Typically these may include:

— production availability for overall subsea system;

— system availability for individual subsystems;

— MFOP;

— component and system reliability prediction;

— identification of early life failures;

— identify high-risk failure modes.

B.7.4.3 Resources and Scheduling

Analysis should be undertaken at the right time, with the right analytical method, consistent with its purpose and the information available at that time. For example:

— System reliability analyses are typically undertaken to determine the system reliability or system availability performance and demonstrate how well the system architecture is meeting the defined performance requirements. Analysis will typically start at concept selection stage and may then be continued through FEED and detail design stages to operation with increasing levels of detail and closer representation of the installed system.

— FMECA studies are typically undertaken to identify system or equipment failure risks and prioritize actions to reduce the likelihood of a failure or reduce its consequences. Early in the design life cycle design detail will be limited, FMECA studies may therefore be performed at a functional level (e.g. during concept selection and FEED). Later in the life cycle more detailed hardware-level FMECA may be carried out (e.g. during detail design stage). The different types of FMECA that may be undertaken include: functional FMECA, qualification FMECA (Q-FMECA), design/hardware FMECA, interface FMECA, P-FMECA, IM-FMECA, and PRS-FMECA.

— HAZID, HAZOP, and P-FMECA may be undertaken to identify hazards and equipment failure risks related to activities such as installation or retrieval of equipment and to identify actions to mitigate risks. These studies should be undertaken in advance of the procedure implementation and with sufficient time to implement any preventive measures identified from the analysis.

B.7.5 Analysis Techniques

Common analytical tools that may be used to support risk and availability analysis include:

1) FMECA;

2) FTA;

3) ETA;

4) importance analysis;

5) RBD;

6) physics of failure and stress strength interference;

7) RAM analysis (system availability analysis);

8) qualitative CCFA;

9) quantitative CCFA;

10) root cause analysis of failure;

11) HAZOP;

12) HAZID;

13) bowtie analysis.

NOTE More detailed quantitative reliability testing analysis techniques (e.g. reliability growth analysis) are addressed in API 17Q.

All input data and models should be realistic and valid representations of the system, its functional failure logic and operating requirements (see B.8).

B.7.6 Additional Guidance

Tables B.3 to B.15 provide additional guidance on each of the analytical tools listed in B.7.5.

Table B.3—FMECA Summary

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, process improvement, further analysis, or testing.
Timing of Application
Due to the versatility of the process, an FMECA can be performed at any stage of a project. However, the focus of the analysis does change depending on when an FMECA is performed.
1) A functional FMECA is performed prior to the definition of specific hardware. The focus of attention is geared toward the functions that the hardware is expected to perform.
2) A hardware/design FMECA is implemented once the hardware has been identified and the assessment can focus on the specific details of the systems/packages/components.
3) An interface FMECA may be implemented once the equipment packages have been identified and focuses on the package and equipment interfaces.
4) A process FMECA is implemented for the specific assessment of the MATIC procedures. The process FMECA is usually performed in terms of the process hardware.
5) An IM-FMECA is implemented prior to or early in operation to identify inspection, monitoring, testing, and maintenance activities to be undertaken as part of the ITMM plan. See Annex D.
6) A Q-FMECA is implemented as part of a new TQP to identify the qualification tests and analysis required to achieve the required TRL and demonstrate required RIM performance.
7) A PRS-FMECA is implemented prior to, or early in, operation to identify potential repair strategies following a failure and the value of investing in spare equipment items.
Procedural Outline Reference: [8]
1) Define the system to be analyzed, including the 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 level based on a worst case consequence scenario related to company risk definitions.
5) For each failure mode, assign a probability of occurrence level.
6) Evaluate the failure modes in relation to the company risk 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) Depending on the type of FMECA, input data may include: drawings of physical system layout, P&IDs, functional performance requirements.
2) Full system definition and operating philosophy.
3) Failure consequence levels.
4) Failure probability levels and associated reliability data.
5) Company risk criticality matrix.
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) May not identify the root cause of the failure mode.
2) Can be a time-consuming task.

Table B.4—FTA Summary

FTA
Objective
1) To logically represent all the possible failure modes of a system or package.
2) To identify the technical cause(s) of the specified failure mode.
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 FEED or detailed 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 an FMECA, i.e. 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: [9]
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 failure mode 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 sub-top event. For each sub-top event, identify the immediate necessary and sufficient causes.
6) Repeat Step 4 and Step 5 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 RCA.
4) Compatible with event trees for cause-consequence analysis.
5) Supports Importance analysis.
6) May be combined with Monte Carlo simulation (MCS) to address event statistical uncertainty.
Weaknesses
1) Complex systems may become difficult to manage and resolve manually.
2) Not suited to the consideration of sequential events.

Table B.5—RBD Summary

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 FMECA is performed.
Procedural Outline Reference: [10] [11]
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). NOTE 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. 6) 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. 7) Logical or numerical assessment of the RBD is best implemented through software.
Input Data Requirements
1) Depending on level of detail and intent: drawings of physical system layout, P&IDs, functional performance requirements. 2) Thorough knowledge of how the system operates. 3) 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 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.6—ETA

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 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 an FMECA is undertaken.
Procedural Outline	Reference: [12]
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 sub-initiating event. For each sub-initiating event, identify all the credible and immediate outcomes from the sub-initiating 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)	Thorough knowledge of how the system operates.
2)	Probability of each branched event. This may require reliability parameters (e.g. hazard rate or Weibull reliability parameters).
3)	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)	May be combined with MCS to address event statistical uncertainty.
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.7—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: [12] [13] [14] [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 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, 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.8—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: [15] [16]
There is no standard procedure for importance analysis. In most cases the importance analysis occurs after one of the other modeling procedures (often, FTA or 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 does not normally require any additional data beyond those used for the modeling/analysis technique to which the importance analysis is to be applied. 2) MCS will require statistical distributions of the data used in the modeling/analysis technique to which the importance analysis is to be applied.
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.9—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 an FMECA or FTA is performed.
Procedural Outline Reference: [15]
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 new 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 that 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 are 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 RCA may get overlooked.

Table B.10—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.

NOTE Common cause failures are of high importance in systems that are relying on redundancy to provide the level of reliability required. This is due to inherent assumptions that the reliability performance of individual component/subsystem are independent of each other. This assumption is typically challenged where; similar items are being used, the same operating procedure is being used for multiple items or the items are in the same or very similar environments.

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: [15]

If the conditional probability of a minimum cut set occurring given that a common cause event X has occurred is $P[M|X]$, then the probability of occurrence of the minimum cut set $P[M]$, is given by:

$$P[M] = P[X]\ P[M|X]$$

where

$P[X]$ is the probability of occurrence of the common cause event.

This is especially applicable for setting reliability requirements when $P[M|X]$ is high and $P[X]$ is a controllable barrier (e.g. failure of subsea electronics system given failure of a seal allowing seawater ingress).

Various methods are available for the quantitative assessment of common cause failures. Data availability determines the level of detail at which the assessment can be performed.

When conditional probabilities are known/accurately estimated, the parametric method can be used.

The beta model is the most commonly used, due to its relative simplicity. There are a number of ways of estimating the beta factor, two of which are briefly explained below.

1) **Beta (β) Method**. Assumes that $P[M|X] = 1$, and requires the failure rate of independent failures, λi, and the failure rate due to common cause factors, λc. The beta factor is then calculated using, $\frac{\lambda c}{\lambda c+\lambda i}$, and can be thought of as the proportion of failures caused by common factors.

$$P[f] = P[f \mid X]\ \beta + P[f|\bar{X}]\ (1 - \beta)$$

2) **Partial Beta (β) Method.** Uses the same methodology as the beta method; however, the beta factor is estimated by summing a number of partial beta values. The partial betas are estimates of groups of factors representing barriers to CCF (e.g. diversity, proximity, complexity, etc.). IEC 61508 provides a 37-question checklist requiring engineering judgement to estimate the different beta factors.

There are a number of other methods ranging in accuracy and simplicity the following lists some of the more common models: the alpha model, multiple Greek letter model, binomial failure rate model, and the boundary model.

Input Data Requirements

1) Failure data for each independent failure event in the minimum cut set.

2) Data on the beta factors or if hard data are unavailable.

3) 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.11—RAM Analysis Summary

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: [16] [12]
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 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 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) Depending on level of detail and intent: drawings of physical system layout, P&IDs, functional performance requirements.
2) Full system definition and operating philosophy.
3) Reliability and maintainability input parameters for every component in the model.
4) Asset operations, maintenance, and intervention strategy.
5) 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) May be combined with MCS to address statistical uncertainty.
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.12—RCA Summary

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: [17]
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 model describing the cause and effect relationships that lead to the event/incident including direct and contributing causes together with 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 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 relies 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. FTA and ETA).
Strengths	
1)	Relates equipment failure to the 12 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.

Table B.13—HAZOP Study Summary

HAZOP

Objectives

1) To identify potential hazards and operating problems that may represent risks to personnel or equipment, or prevent efficient operation.
2) To engage multidisciplinary input through a facilitated set of guidewords to ensure rigor and completeness.
3) To identify actions and safeguards that will reduce, prevent, or mitigate the risk or hazard.

Timing of Application

HAZOP studies can performed at a number of different times within projects and operations.

1) In design to assess system design capability to meet user specifications and integrity requirements.
2) In MATIC to assess the test or installed environment to ensure system is appropriately situated, interfaced, serviced, and contained.
3) In operations to assess procedures and controls to ensure they address the management of hazards for all stages of operation including start-up, standby, normal operation, steady and unsteady states, normal shutdown, emergency shutdown.

Procedural Outline Reference: [18] [19]

1) Define the members of the multi-disciplinary HAZOP team, the objectives, and scope of the HAZOP (including the study boundaries, key interfaces, and key assumptions).
2) Prepare for the study by identifying and agreeing the necessary input data, the template and the guidewords to be used, and the scheduling of the workshop.
3) For the HAZOP workshop process:
   a. Identify all elements (parts or steps) of the system or process to be examined.
   b. Systematically and in order, apply the set of guidewords to each element to evaluate all potential deviations from design intent.
   c. Discuss the causes and consequences of each deviation.
   d. Determine the acceptability of existing safeguards.
   e. Identify, agree, and record any additional actions required to reduce the risk to an acceptable level.
   - It is necessary to consider design intent (and deviations from it) at different stages in the operating life cycle, as well as the risk from operations being performed out of sequence.
   - It may also be helpful to explicitly consider appropriate parameters relevant to the design intent such as flow, temperature, pressure, and composition.
   - Guidewords should be chosen that are appropriate to the study and that are not too specific (limiting ideas and discussion) nor too general (allowing loss of focus).
4) The HAZOP workshop should be recorded in the agreed HAZOP worksheet along with agreed follow-up actions.

Input Data Requirements

1) Full system/process definition drawings, design basis, and operating manuals.
2) Agreed HAZOP guidewords and template.

Strengths

1) Systematic and comprehensive methodology providing a rigorous analysis of a system and its operation.
2) Simple and intuitive process based on a well-defined procedure.
3) Supports the identification of hazards that are difficult to detect, analyze, isolate, count, predict, or rooted in human performance and behaviors.

Weaknesses

1) No means to assess hazards involving interactions between different parts of a system or process.
2) No formal means of assessing risk ranking or effectiveness of safeguards, although this could be added in.
3) Hazard identification is sensitive to the choice of guidewords. Some design weaknesses may be missed.

Table B.14—HAZID Summary

HAZID
Objective
1) To identify all possible hazards (process and nonprocess) associated with the operation of a system or system intervention that would influence health, safety, or the environment. 2) To identify all possible consequences and escalations of the hazard. 3) To prioritize areas for introducing safeguards in system design, operation, or intervention including improved ITMM activities for risk reduction.
Timing of Application
1) A HAZID is a process for early identification of hazards and may be used early in a project as soon as process flow diagrams, etc. are available. It may be revisited at any stage throughout design, MATIC, or early in operation to review and update the assessment and actions.
Procedural Outline Reference: [20]
1) Define and agree with the HAZID team the scope of system to be analyzed, including: internal and interface functions/hardware, performance expectations, and definitions of failure. 2) Logic block diagrams can be useful to represent system or procedures inter-dependencies and inter-relationships. 3) For each system item, interface, or procedure step, use guidewords/checklists to identify all potential hazards, their causes, and immediate effects on the system, operation, or implementation of the procedure. 4) For each hazard, identify existing and additional safeguards including means of detection and other compensating provisions required to remove or mitigate the risk. 5) If required, risk can be quantified in terms of severity and likelihood and reassessed to account for selected mitigations. 6) HAZID output including arising actions should be recorded and managed for continued risk management.
Data Requirements
1) Initial system/process definition dependent on maturity of the design, but likely to include P&IDs and the design basis. 2) Agreed HAZID checklist/guidewords and template.
Strengths
1) Facilitates early identification of hazards to enable early mitigation before costs escalate. 2) Versatile; applicable to systems, components, and procedures at all project stages. 3) Systematic identification and prioritization of areas of operation weakness.
Weaknesses
1) If carried out very early and not maintained, the information can become outdated and become an irrelevant input to engineering and risk management decisions.

Table B.15—Barrier/Bowtie Analysis

Barrier/Bowtie Analysis
Objective
1) To communicate the management of risk for a system. 2) Demonstrate relationships between causes, consequences, and barriers used to manage and control risk.
Timing of Application
1) Barrier/bowtie analysis may be applied at any time throughout the life cycle from concept selection (once a design has been decided upon) through to operations.
Procedural Outline Reference: [20] [21]
1) Define the hazard to be managed (e.g. loss of containment) and the event causing the hazard to be realized (e.g. pipeline rupture). The event becomes the knot at the center of the bowtie. 2) Identify threats and causes of the event (left-hand side of the bowtie). 3) Identify consequences should the hazard be realized (right-hand side of the bowtie). 4) Determine preventative barriers to remove or reduce the likelihood of the hazard and for each barrier, identify root causes of failure and determine actions to control and prevent hazard realization. 5) Determine barriers to mitigate the consequences of the hazard (recovery preparedness measure) and for each barrier identify escalation factors and controls and preventive actions.
Input Data Requirements
1) HAZOP or HAZID to identify the threat and trigger for the knot of the bowtie. FTA to determine the cause side of the bowtie. ETA to determine the consequence side of the bowtie.
Strengths
1) A highly effective visual means of displaying system risks (hazards causes and consequences) how they are to be managed (barriers to prevent hazards being realized or the consequences of hazards being realized). Can be linked to FMECA output. 2) Addresses all risks, not just safety or environmental risks. It facilitates risk reduction and helps to identify where resources should be focused for hazard prevention and mitigation. 3) Cause-consequence tools may be used to quantify bowties. 4) Provides an audit trail; the diagrams and critical tasks provide protocols around which auditing can be performed.
Weaknesses
1) Bowtie tools are qualitative or semi-quantitative unless undertaken using FTA and ETA. 2) Depends on experience of personnel and active workforce involvement.

B.8 KP 6—Verification and Validation

B.8.1 Objectives and Preparation for KP 6

Verification and validation are procedures performed during projects and operations to confirm that any given activity is the correct one and that it has been carried out correctly.

B.8.2 Recommendation for Senior Management

— Create high-level process document covering management expectations and procedures for verification and validation to address resourcing and degree of independence from the project.

— Integrate verification and validation guidance/processes into project and product design execution.

— Provide for verification and validation training as needed.

B.8.3 Recommendation for Project and Operations Management

— All project reliability and integrity activities should be subject to a formal verification process to ensure conformance to specification.

— Identify all activities that require validation. Particular attention should be paid to activities related to:

  — setting of goals and requirements (KP 1);

  — design for reliability and integrity (KP 3);

  — qualification of technology (KP 8);

  — quantitative risk and reliability assessments (KP 5);

  — performance tracking and data management (KP 9).

— Identify resources and competencies needed for verification and validation in the project, with due regard to the size, scope, and nature of the work to be undertaken. Refer to company management practice document requirements:

  — address verification and validation requirements during planning and organizing of project reliability and integrity activities (see KP 2);

  — higher levels of verification and validation effort will be required in projects with high levels of technical risk (e.g. TRC A or TRC B);

  — where verification and validation of project activities are required, identify the validation/verification authorities to be used.

B.8.4 Process Description

B.8.4.1 Verification

The verification process is a review by competent but independent personnel to provide confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g. the requirements for a specific test have been implemented).

B.8.4.2 Validation

Validation is the process of confirming, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled (e.g. the correct test has been selected). It should ascertain the appropriateness of data, assumptions, or techniques in terms of the objectives of both the RIM strategy and the individual RIM 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, especially quantitative models and simulations, should be validated to ensure that they based on sound underling principles and are generating results that 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).

B.8.5 Additional Guidance

B.8.5.1 Validation Activities

Example questions that may be addressed during the validation process are presented below.

— **TRC.**

  — Has a TRC workshop activity been completed at an appropriate time in relation to the project schedule?

  — Is the TRC category identified by the team valid for the project’s scope, scale, and complexity and the technology involved?

— **Setting of Goals and Requirements.**

  — Have valid goals and requirements been defined for system reliability, availability, and integrity?

  — Are the project defined reliability, availability, and integrity goals and requirements consistent with the company’s objectives?

  — Are the goals and requirements, clearly defined, measurable, and realistically achievable within the constraints of the project?

— **Design for and Deliver Reliability and Integrity.**

  — Are suitable reliability improvement techniques being implemented?

  — Are suitable integrity management techniques being implemented?

  — Are appropriate maintainability designs being considered?

— **Qualification.**

  — Is the correct test being specified given the desired results of the test?

— **Analysis.**

  — Is the correct analysis tool being implemented given the required results?

- Is the correct model being used?
- Is the model being populated with the right data?

- **Performance Tracking and Data Management.**
  - Are suitable data acquisition techniques being applied?
  - Are the data analysis techniques being used appropriate for managing reliability, availability, and risk in operations and for future projects?

B.8.5.2 Application of Verification and Validation to Project Activities

Verification and validation is complementary to and applicable to all KPs within the strategy.

Verification and validation is an important underlying process, when considering the confidence and value of the evidence presented within the RIAD.

Verification and validation activities are best conducted via peer review independent of the project delivery team. If independent expertise cannot be found within the company or where internal expertise is limited, projects may choose to employ an external authority (an external organization or consultant) for validation and verification.

The importance and required effort of this key task increases with the associated level of risk. All processes and tasks should be verified and validated to ensure that they have been implemented correctly.

B.9 KP 7—Project Risk Management (PRM)

B.9.1 Objectives and Preparation for KP 7

The PRM process encapsulates the set of integrated management actions and procedures required to effectively manage the risks to a project's and operation's budget and schedule arising from activities generated by the reliability and integrity work scope in the project. This will include ensuring that conflicting project and operations requirements and goals are resolved and do not compromise the overall RIM achievement.

B.9.2 Recommendation for Senior Management

- Provide clear and unambiguous guidance on the balance to be struck between delivering a project to predefined budgets and schedules and delivering acceptable reliability, maintainability, and integrity performance in operations.
- Define expectations and provide resources for the creation of a process for project and operations risk management. This should include and address technical risks.
- Create high-level good PRM practice documents covering management expectations and procedures for managing emergent risks in projects and operations.
- Provide training to ensure PRM process can be translated into PRM practice.
- Ensure sufficient resources are available to perform reliability and integrity assessments and to respond to actions.
- Define and agree the authority level for project managers to respond to emerging RIM risks during projects and operations.

B.9.3 Recommendation for Projects and Operations Management

— Ensure PRM is consistent with company guidance. Ideally, the project manager should be aiming to ensure that reliability and integrity objectives and deliverables are not compromised by budget and schedule constraints.

— Work with senior managers to ensure that budgets and project schedule are realistically achievable.

— Ensure that all emergent risks to the project and operation success are identified, assessed, and managed.

— Ensure that reliability and integrity activities are undertaken at the right time with the right tools and competent reliability engineering resource.

NOTE Realization of faults and reliability/integrity problems late in the design process leads to more rapid escalation of correction/rectification costs than those found early in the project.

B.9.4 Process Description

Few, if any, subsea projects are repeats of previous projects. While most projects do contain a number of repeated elements, each project will have its own unique risks. Additional effort may be required to understand the technical risks and deliver acceptable system reliability and integrity performance.

PRM is undertaken throughout the whole project and operations life cycle (or field upgrades during operations) to enable all risks to be identified, quantified, managed, and where practicable, eliminated.

PRM should ensure that the project and operational goals are fully aligned with overall business performance and regulatory objectives and provide the focus for delivery of reliability and integrity goals and requirements.

PRM should ensure that CAPEX does not adversely affect OPEX.

B.9.5 Additional Guidance

B.9.5.1 Formal Project Risk Analysis

All projects and operations should undertake a formal assessment of risks to budget and schedule arising from reliability and integrity activities. In most cases it is likely that the risk analysis will be qualitative. This should be undertaken early in projects and operations, and updated at the start of each project stage and, when required, during operations.

Project risk analysis involves the following stages.

1. **Risk Review.** Review the project plan overall and projected reliability and integrity activities plans identified in KP 2. Project risk reviews are a component of good project management practice; reference should be made to relevant company documentation. Alternatively, reference should be made to BS IEC 62198:2001 for guidance on the application of PRM.

2. **Risk Response Analysis.** Assess the risk to project budget and schedule introduced by scheduling reliability and integrity activities into the project.

    — Step 1: List all the reliability and integrity tasks to be performed and known at the time.

    — Step 2: Identify applicable project risk categories, e.g.:

        — cost;

  - schedule;
  - safety;
  - supply chain.
- Step 3: Identify project risks associated with reliability and integrity activities.
- Step 4: Assign risks to the identified categories and assess uncertainties.
- Step 5: Identify the risks (likelihood together with severity of impact/consequence).
- Step 6: Identify responses to project risks.
- Step 7: Update the project risk register to incorporate the identified risks and responses.

B.10 KP 8—Qualification of Technology

B.10.1 Objectives and Preparation for KP 8

Qualification is the process by which systems are examined and evidence is provided to demonstrate that the technology meets the specified requirements for the intended use.

B.10.2 Recommendations for Senior Management

The following general technology qualification activities are recommended for senior management.

- Define expectations and a process for the management of technology qualification in projects and operations. This should address provision of:
  - procedures for assessment of technology readiness;
  - internal or external equipment and test specialists;
  - templates for identification of qualification requirements (e.g. Q-FMECA);
  - templates for reporting results of qualification activities.
- Define expectations and provide resources for the creation of guidance or good-practice documents that describe the TQP.
- Provide access to relevant training for project and operations teams on the qualification process to be used by projects.

B.10.3 Recommendations for Project and Operations Management

- Ensure that company technology qualification practice is followed.
- Ensure sufficient resources are allocated for completion of technology qualification activities within the project schedule and budgetary constraints.
- Ensure sufficient resources are allocated to inspection and monitoring during operations for completion of technology qualification activities to achieve TRL 7.

B.10.4 Process Description

B.10.4.1 General

New technology qualification is particularly important at the design stage but may be required at any stage of the asset life cycle including operations (e.g. updating existing equipment with new technology packages) and decommissioning (e.g. using new technology equipment as part of the decommissioning process).

The extent to which equipment is qualified for a particular application should be formally assessed to define its readiness for field operation through its TRL.

B.10.4.2 TRL

TRL is a measure of the extent to which an item of equipment is qualified for a particular application.

Eight TRLs have been defined ranging from a minimum of TRL 0 to TRL 7 as follows.

— TRL 0—Basic Research: Basic R&D paper concept;

— TRL 1—Concept Selection: Proof of concept as a paper study or R&D experiments;

— TRL 2—Concept Demonstration: Experimental proof of concept using physical model tests;

— TRL 3—Prototype Development: System function, performance, and reliability tested;

— TRL 4—Product Validation: Pre-production system validated and environment tested;

— TRL 5—System Integration Testing: Production system interface tested;

— TRL 6—System Installed: Production system installed and tested;

— TRL7—System Operation: Production system field proven.

Details on the TRL ladder and qualification expectations at each TRL are provided in API 17Q.

During a field development project, the project team should assess the TRL of equipment prior to procurement to check whether:

— the equipment is sufficiently qualified for application in the project;

— the equipment can be qualified to the required TRL within the time frame of the project.

Equipment developers may be required to assess the TRL of their equipment for a specific application in collaboration with an operator to confirm that equipment is ready for application in the field or gauge the level of qualification effort needed in a TQP to raise the TRL from the initial level to its required level.

Both initial and required TRLs should be determined for a given item of equipment. This should be used as the initiation of the new TQP, the aim being to raise the TRL from its initial value to the required TRL.

B.10.4.3 Technology Qualification

All equipment to be used subsea, regardless of system design or application, should be qualified to a TRL that ensures that equipment will function reliably in operation and meet defined reliability and integrity requirements. This is particularly important for new technology or for equipment based on existing technology to be operated outside previous operating experience.

In this RP a distinction is made between standard qualification programs (SQPs) and new technology qualification involving a formal TQP. The latter will usually require a greater degree of testing and analysis effort to demonstrate that the equipment will meet specified reliability and integrity requirements.

The decision to implement a new TQP or SQP depends on the degree of novelty or change involved in the design, manufacture or operation of equipment. Further details regarding TQP and SQP can be found in API 17Q.

B.10.4.4 New Technology Qualification Programs

For equipment to be qualified using a TQP, 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 current TRL, and the required TRL.

The impact of the TQP on the project schedule, or the timing of introduction into operations, may be significant. Where new technology is to be introduced in a project with significant remaining qualification work to be completed, the Operator should aim for a flexible schedule with sufficient resources to handle unexpected consequences arising from tests and to ensure completion of qualification prior to operation. The qualification plan should be aligned with the reliability and integrity plan where there are common tasks.

The major part of equipment qualification effort should be undertaken outside of the project environment and undertaken within a separate product development project. This may be led by the operator with OEM support or led by the OEM with operator support.

An outline TQP, showing how this relates to the DPIEF reliability assurance loop, is shown in Figure B.5.

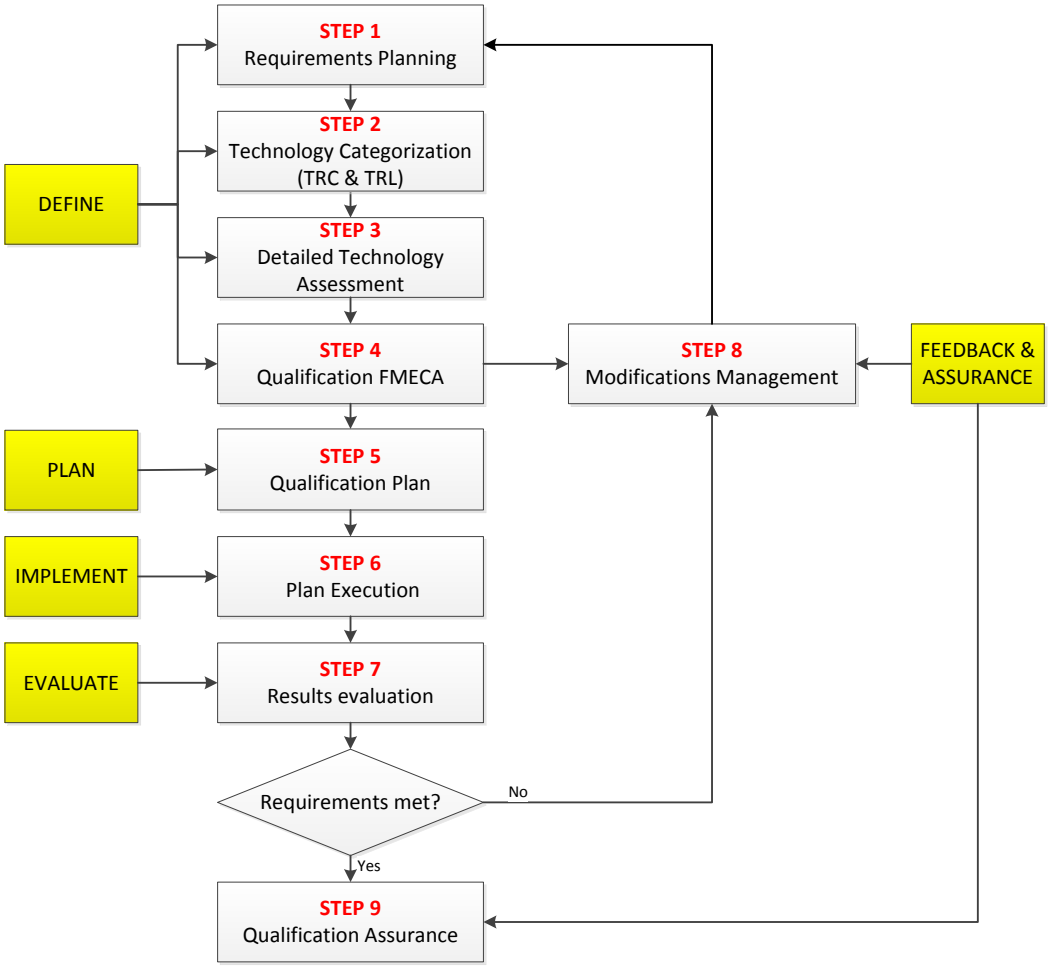


Figure B.5—Outline TQP

The key elements of a TQP are as follows.

Step 1. Requirements Planning

Define the goals and requirements for the technology and its application together with qualification requirements.

Step 2. Technology Categorization

This step is a high-level categorization using TRC and TRL to identify the qualification approach (TQP or SQP) to be adopted.

Step 3. Detailed Technology Assessment

Develop a practical system taxonomy and undertake a detailed assessment of TRL and performance goals and requirements in preparation for FMECA. The level of system indenture (level of detail) should be consistent with the testing and analysis activities needed to qualify the equipment.

Step 4. Qualification FMECA

The FMECA should be used to support identification and development of the qualification plan (Step 5). The intent is that every qualification activity is traceable to specific rows in the FMECA. The FMECA output may also identify design improvements to be made before testing commences.

Step 5. Qualification Plan

Develop a detailed qualification plan, including required analysis and testing activities, traceable to the Q-FMECA, together with required resources, schedule, and procedures including acceptance criteria to meet the specified goals and requirements. The plan should be validated to confirm that the qualification activities will provide appropriate evidence of the extent to which goals and requirements will be achieved.

Step 6. Plan Execution

The execution of qualification test plans will typically include both modeling activities (engineering analyses or reliability analyses) and physical testing activities together with appropriate verification. Plan execution should ensure that the required raw data are generated and recorded ready for evaluation.

Step 7. Results Evaluation

Once qualification activities are underway, the generated data, e.g. test data or analysis results, should be assessed and evaluated against the specified goals and requirements.

Step 8. Modifications Management

If the test results indicate that the technology is not meeting the specified requirements, then design improvements may be required.

Step 9. Qualification Assurance

The final step in the TQP is the documentation of qualification claims together with associated arguments and evidence of qualification achievements in the qualification assurance document.

More information on the TQP and TRLs can be found in API 17Q.

B.11 KP 9—Performance Tracking and Data Management

B.11.1 Objectives and Preparation for KP 9

Asset performance predictions can only be made if RIM data are available to support analysis. Confidence in the output of the assessments requires the RIM data to be relevant, accurate, and statistically significant.

The objective of KP 9 is to collect and organize reliability and integrity performance data and enable the operator of an asset to demonstrate the extent to which reliability and integrity performance goals and requirements are being met.

B.11.2 Recommendation for Senior Management

With regard to reliability, availability, maintainability, and integrity performance tracking and data management:

- define high-level company goals and requirements;
- define expectations and provide resources for the creation of supporting documentation that defines scope and procedures and sets out the company's policy and position for its achievement in operations and for its feedback to project teams and suppliers;
- define competency requirements for data collection and analysis by central engineering teams and by operations teams;
- define expectations and provide resources for the creation of a process with practical procedures and tools for data collection, analysis, and communication in operations that conforms to agreed industry standards;
- define expectations and provide resources for the creation or procurement of facilities and tools including:
  - computer-based data management system, for recording, collating, and analyzing data;
  - availability of analytical tools including: RCA and statistical data analysis tools;
- define expectations and provide resources for the creation of procedures for comparing and aligning project predictions with operational achievements;
- define expectations and provide resources for the creation of procedures for continuous improvement of the database and access to relevant data for analysis by current and future projects and operations;
- define the authority level for decision-making.

B.11.3 Recommendations for Project and Operations Management

With regard to reliability, availability, maintainability, and integrity:

- define data and documentation requirements for handover to operations;
- develop an effective data management system to support information handover to operations;
- develop an equipment hierarchy or taxonomy that is a realistic representation of the installed system;
- collect, track, and manage data in accordance with the specified company requirements;

— check that data are collected at the required level of system granularity in accordance with defined system taxonomy, company requirements, and industry-accepted practice;

— analyze data and track performance to:

  — demonstrate continuous improvement;

  — detect deterioration in performance;

  — detect changes in failure occurrence patterns (e.g. due to common cause failures);

  — demonstrate alignment between project predictions and operational achievements;

— ensure that the need for accurate data collection and analysis is fully understood and supported by both the operations and project teams;

— ensure the staff involved in data collection and analyses are appropriately trained and competent in the required tools and methods and are able to accurately record the required data ready for incorporation into the database.

B.11.4 Process Description

B.11.4.1 General

NOTE In this key process, the use of the term *RIM data* implies and encompasses data for reliability, availability, maintainability, and integrity. Where reference is made to a specific type of data such as reliability data or integrity data, the specific term is used.

A key driver for reliability improvement is better understanding of failure mechanisms and root causes. 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 defects during testing. Equipment failures can also be the result of a different environment to that assumed in design, design errors, or inadequate design processes. As recognized in ISO 14224, it is essential to be able to capture these data and create a failure database including lesson learned as shown in Figure B.6.

It is also important to develop an equipment hierarchy or taxonomy that is a realistic representation of the installed system. 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 provides a suitable taxonomy on which to base the data collection process.

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 contracting strategy, MOC, etc. so that the sensitivity of related specific failure events, mechanisms, and root causes to these parameters can be revealed.

Figure B.6 outlines the intent of a reliability data collection system. Data related to failures and maintenance action occurring prior to MATIC stage and during operations, up to and including decommissioning stage, should be collected. The raw data, which typically includes equipment type, failure mode, time in operation, time to restore to operation, etc., but which may include more detailed information, should be stored in a suitable database such that it can be retrieved for analysis to determine the key RIM parameters (failure rate and MTTR) that are used to support system reliability and integrity analysis and decision-making throughout the life cycle.

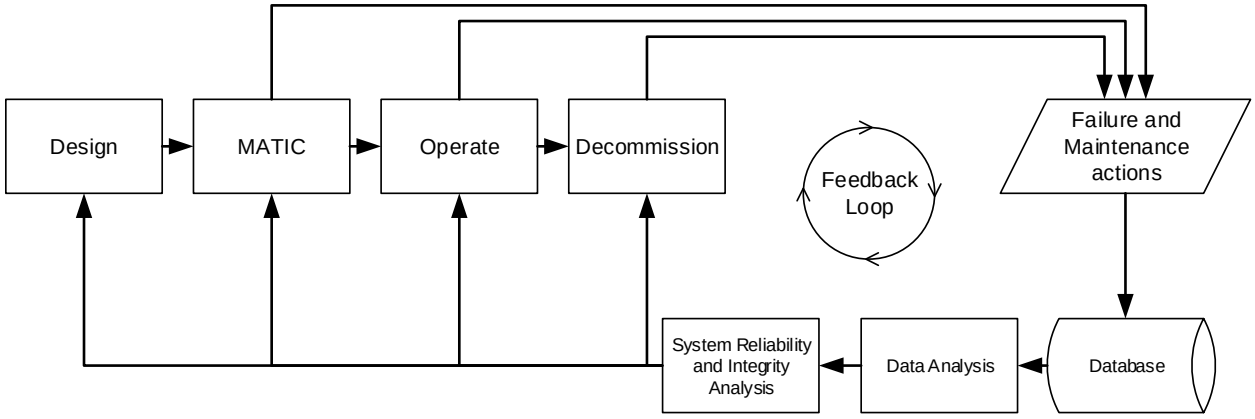


Figure B.6—Data Collection and Usage Strategy

CM is the process that identifies, defines, prepares, controls, dispositions, and archives information and data relating to the system's design, architecture, procedures, results of analyses, etc. This includes updating data and information when changes are made (i.e. following an MOC process; see KP 11).

This should be seen as a continuous process throughout the asset life cycle that ensures that the most up-to-date information is available to support planning, analysis and decision-making.

For example, a CM activity might record a new subsea facility configuration (e.g. the way chemical injection was routed into a manifold or tree following the blockage of an umbilical core) and ensure all related documents and data are updated in light of the change.

B.11.5 Additional Guidance

B.11.5.1 Data Management During the Asset Life Cycle

Subsea installations are expected to achieve a level of reliability and integrity performance during operations that meet the requirements of the operator and the regulator. Demonstrating that the requirements are being met requires the field performance to be measured.

In meeting the RIM objectives set by this process, the entire life cycle should be considered.

During Product Development Projects. To support assessment and measurement of product RIM performance and technology qualification, suppliers should do the following.

— Identify and assess reliability data at component or parts level to support estimation of equipment reliability or availability performance using appropriate tools (see KP 5). Component and parts reliability data will likely come from sources other than field data collected by field operators.

— Measure equipment reliability and integrity performance through testing and reliability growth programs undertaken during TQPs.

— Assess FMECA. This may be communicated to end users to support analyses performed by projects and operations.

— Establish communication procedures with end users of supplied equipment to facilitate feedback of field RIM performance as an input into supplier's reliability improvement program.

During Field Development Projects. To support project stage assessments and analyses, project teams should ensure that appropriate RIM data are identified from the data sources available (see Table B.16).

— Collect RIM data during factory acceptance test (FAT), system integration test (SIT), installation, and commissioning to support required analyses prior to or during operation.

— Record any changes to system configuration equipment or procedures identified during commissioning, and update the RIAD accordingly.

— Put appropriate preparations in place for tracking and managing RIM data during field operation (see B.11.1).

— Identify data needed to support the integrity management program (ITMM tasks). These data are key inputs to decision-making to enable the operator to improve and control overall installation performance and installed equipment performance.

— Perform gap assessment:

  — consider baseline ITMM tasks needed prior to operation (see Annex D);

  — identify data gaps;

  — access the required data;

  — verify that the required data are documented and available to projects and operations in the operator's RIM data management system.

— All RIM data generated from analyses performed during the field development project should be referenced in the overall RIAD.

During Operations. To support measurement and analysis of field performance, the operations team should:

— collect RIM data in conformance with the company requirements subject to field and operational constraints and combine with earlier data collected;

— pay particular attention to monitoring and data collection in the early life period;

— drive for reliability growth in the early life period (use reliability growth analysis);

— sustain the inherent reliability of the field through an effective maintenance strategy.

B.11.5.2 Integrity Management and Field Performance Data

Knowledge management is key to effective reliability and integrity management, organizational learning (KP 12), and life extensions. Analysis of field data leads to greater knowledge of equipment performance and hence to improved system performance.

Data collected should include the following.

— **Equipment Data.** This may also include design parameters that set the acceptance (anomaly) criteria for the ability of the equipment to perform required functions. These data may be found in design reports for the system and validated during fabrication, installation, and commissioning test reports. Ideally a complete design, fabrication and installation dossier should be made available, summarizing all pertinent data for the subsea system.

Table B.16—Data Sources

Data Source	Equipment	Available From
OREDA handbooks	Process equipment (offshore)	DNV GL, Veritasveien 1, 1363 Hovik, Norway, www.dnvgl.com
MIL-HDBK-217F—*Reliability Prediction of Electronic Equipment*	Electronic components	U.S. Military Handbook
EPRD—*Electronic Parts Reliability Data*	Electronic components	RIAC Quanterion, 100 Seymour Road, Kunsela Hall, Suite C106, Utica, NY 13502
NPRD—*Nonelectronic Parts Reliability Data*	Mechanical and electromechanical components	RIAC Quanterion, 100 Seymour Road, Kunsela Hall, Suite C106, Utica, NY 13502
PDS Data Handbook	Sensors, detectors, valves, and control logic	Sydvest, Sluppenvegen 12E, 7037 Trondheim, Norway
IEEE 493-1997	Electrical power generation and distribution	ISBN1-55937-066-1
STF18 A83002, *Reliability of Surface Controlled Subsurface Safety Valves*	Surface controlled subsurface safety valves	Exprosoft, 7465 Trondheim, Norway, www.exprosoft.com
STF75 A89054, *Subsea BOP Systems, Reliability and Testing. Phase V*	Subsea blowout preventers	Exprosoft, 7465 Trondheim, Norway, www.exprosoft.com
STF75 A92026, *Reliability of Surface Blowout Preventers (BOPs)*	Surface blowout preventers	Exprosoft, 7465 Trondheim, Norway, www.exprosoft.com
STF38 A99426, *Reliability of Subsea BOP Systems for Deepwater Application, Phase II DW*	Subsea blowout preventers—deepwater subsea	Exprosoft, 7465 Trondheim, Norway, www.exprosoft.com
SubseaMaster & WellMaster	Components in oil wells (BOPs and SCSSVs)	Exprosoft, 7465 Trondheim, Norway, www.exprosoft.com
EIREDA Database European Industry Reliability Data Handbook, Electrical Power Plants	Valves, sensors and control logic (nuclear power station data)	EUROSTAT, Paris
Pipeline and Riser Loss of Containment (PARLOC) Report	Pipelines and Risers	Oil & Gas UK, 6th Floor East, Portland House, Bressenden Place, London SW1E 5BH, UK

NOTE The criteria are important in defining whether an item of equipment is in the failed state, degraded (but functioning) state, or working state.

— **Field Data.** Subsea field data may be collected in the following broad ways.

  — Inspection:

    — external general visual inspection (e.g. by ROV);

    — internal ILI (e.g. using intelligent pigging tools).

  — Testing (e.g. valve timing tests, valve leakage tests).

  — Sampling (e.g. production or hydraulic fluids).

  — Process monitoring (e.g. MPFM, pressure, and temperatures of production fluids).

  — Condition monitoring (e.g. corrosion, leakage, vibration, stress, hydraulic fluid composition, etc.).

— **Baseline Data.** For inspection, testing, sampling, and condition monitoring to be effective a baseline, setting the initial conditions of the component/package, should be defined.

Failure and maintenance reliability data collection should encompass data relating to all of the installed equipment within the boundaries described in API 17A and in accordance with the requirements of ISO 14224.

Data to be collected may be categorized under four main headings (shown in bold below):

— **equipment data** (design);

— **application data** (usage);

— in-service data:

  — **failure data:** mode, mechanism, root cause, time to failure;

  — **maintenance data:** time to restore, type of maintenance action taken; preventive, corrective, opportunistic, type/method of intervention.

B.11.5.3 Strategy for RIM Data Collection

A strategy for RIM data collection is summarized in and described 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 (e.g. the design and manufacturing data).

   b) Installation data should be captured by the equipment supplier if equipment is installed directly by the supplier. If equipment is installed by an installation contractor, the installation data should be captured by the operator or the installation contractor working with the operator.

   c) Operators are responsible for collection of the application aspects of the equipment data (e.g. time of failure, usage, environmental aspects, process conditions, locations, etc.).

   d) There is necessarily joint responsibility for failure analysis. For example, the operator should provide data relating to time, place, and circumstances of failure; manufacturer provides input to RCA data during investigation.

The organization responsible for collecting the data should be 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. This organization should consider obsolescence in respect to data storage reader hardware.

B.11.5.4 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 envelopes for the operator, and helping direct improvement efforts for future systems.

Typical information to be collected will include:

— equipment type;

— serial number;

— material specifications;

— manufacturing processes (e.g. welding procedures, treatment processes, if used, etc.);

— applicable design code;

— equipment application rating (e.g. pressure, temperature rating, etc.);

— equipment description (e.g. part numbers);

— FAT/SIT results;

— qualification tests results;

— lessons learned.

B.11.5.5 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 [e.g. flow rate, pressures, sand production, water production, gas-oil ratio (GOR), fluid composition, etc.];

— geographical location, including water depth, and relevant metocean data;

— equipment in-service information (storage of equipment, out of service, batch installation, etc.);

— failure data, as described in B.11.5.2;

— maintenance data, if equipment is taken out of service, replaced or adjusted;

— MOC (equipment application changed, change of service).

B.11.5.6 Failure Detection and Monitoring

B.11.5.6.1 General

Operators, working with equipment suppliers, should undertake a detailed analysis of the equipment and/or system failure modes and mechanisms to determine the best available means to:

— confirm the status of equipment and/or system (detect failure and time of failure);

— identify and track deterioration in function or performance of equipment and/or system prior to failure;

— identify when deterioration may require corrective action.

FMECA or RCM analysis may be used to support identification/confirmation of the most appropriate method for detecting failure and deterioration of functions. For instance, an FMECA may be used by asking specific questions such as the following.

— Component function and functional failure mode: can this be directly or indirectly monitored?

— Failure mechanisms and causes: can these be monitored or measured?

— Failure effects and consequences (local or global): can these be detected or measured?

Analyses undertaken during design should address these aspects. However, they should also be included in analyses undertaken by the operations team (e.g. IM-FMECA)—this is particularly important for older assets for which design FMECAs may not have been undertaken or be available.

The requirement for an effective method for failure detection or condition monitoring will depend on a number of factors including;

— the risk of the failure (i.e. the consequence and frequency of occurrence);

— whether the failure is evident to the operator or not (revealed or unrevealed failure);

— whether additional compensating provisions are available or not.

For example, if the failure mode under consideration is an unrevealed failure and the consequences of the failure have significant health, safety, environmental, or financial implications, then this should drive the requirement for an effective periodic testing regime. Ideally this testing would be conducted in such a way as to support condition monitoring of the item.

The outcome of the FMECA or RCM analysis will be the selection of the most appropriate means of data collection, e.g. through:

— inspection (to detect damage or deterioration);

— equipment testing (to confirm functional capability of active or standby equipment, e.g. valves);

— condition monitoring (instrumented monitoring system and signature monitoring);

— process monitoring (temperature, pressure, flow, fluid sampling).

These data may be used to inform decisions between maintenance and integrity management actions such as

— condition-based maintenance: repair or replace when condition reaches a defined limit;

— scheduled maintenance: undertake maintenance action at specified times (e.g. marine growth cleaning, bolt tightening, etc.);

— scheduled replacements: replace equipment when a specific age is reached;

— run to failure: repair or replace equipment when failed.

B.11.5.6.2 Signature Monitoring

All systems have a normal signature that should be monitored. For example, this approach may be applied to monitoring pressure-time transients for valves during opening or closing. 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.

B.11.5.7 RIM Data Analysis

B.11.5.7.1 General

All system and equipment failures should be collected and collated for analysis. Operators are encouraged to share failure data with each other and with their equipment supplies.

B.11.5.7.2 Generic Data

Most operators use outside organizations to collate their failure data, estimate failure rates, and build a shared reliability database. OREDA, which is based on the reliability data management standard ISO 14224, is the best known and most widely used.

For those operators that belong to the OREDA joint industry project, RM data are available to operators as an electronic OREDA database. A subset of the full OREDA dataset is available to users outside the OREDA in the form of data handbooks that are published periodically.

B.11.5.7.3 Field-specific Data for Equipment

Data for failures occurring on specific installations have particular relevance to operations and the management of integrity.

Therefore where field specific data are available, field data should be analyzed to determine the failure pattern and ascertain trends. For example, an increasing failure rate would indicate deterioration in equipment field performance and a decreasing failure rate would indicate reliability growth.

B.11.5.7.4 Field-specific Production Availability

Production availability forecasts undertaken during projects should be updated early in operations and then on a regular basis thereafter. The update should take account of:

— actual installed hardware;

— actual operating activities;

— observed failure rates.

The updated field production availabilities may be then used to:

— update the integrity management program;

— update spares holding requirements;

— forecast future maintenance and intervention costs and LCCs;

— forecast future deferred production costs and net present value (NPV).

B.11.5.7.5 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? These data can be used to modify life expectancy under similar operating regimes and in similar environments for equipment in current operation or for new equipment.

B.12 KP 10—Supply Chain Management

B.12.1 Objectives and Preparation for KP 10

The objective of KP 10 is to ensure that reliability, integrity, and technical risk management goals, requirements, achievements, and lessons learned are communicated to equipment and service suppliers to projects and operations.

B.12.2 Recommendation for Senior Management

— Define expectations and provide resources for the creation of a process for supply chain management for projects and operations to address:

  — identification, selection, and auditing of suppliers;

  - specification of reliability and integrity goals and requirement to suppliers.

- Define expectations and provide resources for the creation of guidance documents with:
  - templates for reliability and integrity specification;
  - procedures for assessing supplier capability;
  - strategy and procedures for obsolescence management.

B.12.3 Recommendations for Project and Operations Management

- Ensure reliability and integrity goals and requirements are included in equipment or service supplier specifications.
- Ensure obsolescence plans are in place for the project.
- Ensure reliability and integrity capability have been assessed prior to selection of equipment or service suppliers.

B.12.4 Process Description

B.12.4.1 General

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 and integrity goals and 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.12.4.2 Organizational RCMM Audits

The ability of an organization to achieve the goals and requirements set within the resource constraints established will depend on the reliability and integrity capability maturity of the organization undertaking the relevant task. This includes the timely and adequate completion of reliability and integrity activities related to the 12 KPs. Organizational RCMM audits can be applied to any organization within the supply chain including operators, engineering contractors, and equipment vendors. In the case of a supplier organization, this will usually be restricted to equipment within the supplier’s scope of supply.

The active assessment and selection of vendors and contractors occurs during the FEED and detailed design stages. However, the concept of reliability and integrity capability maturity should be considered throughout the project planning stages and operations, 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.17.

Table B.17—Overview of RCMM Levels

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

Reliability and integrity capability audit 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 and integrity 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.

— Audits during supplier/contractor selection should be conducted as a high-level review of the potential supplier/contractor with specific regard to the reliability and integrity specification. This type of assessment may form part of the customer's specification by requesting evidence/statements of capability.

— Full audits may be conducted as part of a project to assess, in real time, the supplier/contractor reliability and integrity capability. This may be viewed as an update or verification of the supplier/contractor capability conducted outside of the project environment.

Reliability and integrity audits are applicable to all organizations in the supply chain; however, typically they are used by operators assessing first tier suppliers and first tier suppliers assessing higher tier suppliers in their supply chain.

In the case of the latter, the audit should place emphasis on MOC process through the supply chain. A simplified approach to the assessment procedure is provided below. A more detailed description of the process is outside the scope of this RP.

— Define the elements of the KPs required for the reliability and integrity 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 and integrity capability maturity level 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 each KP and the overall reliability capability maturity levels.

— Compare against required reliability and integrity capability maturity levels (e.g. with a spider diagram; see Figure B.7).

— Document recommendations and follow-up actions.

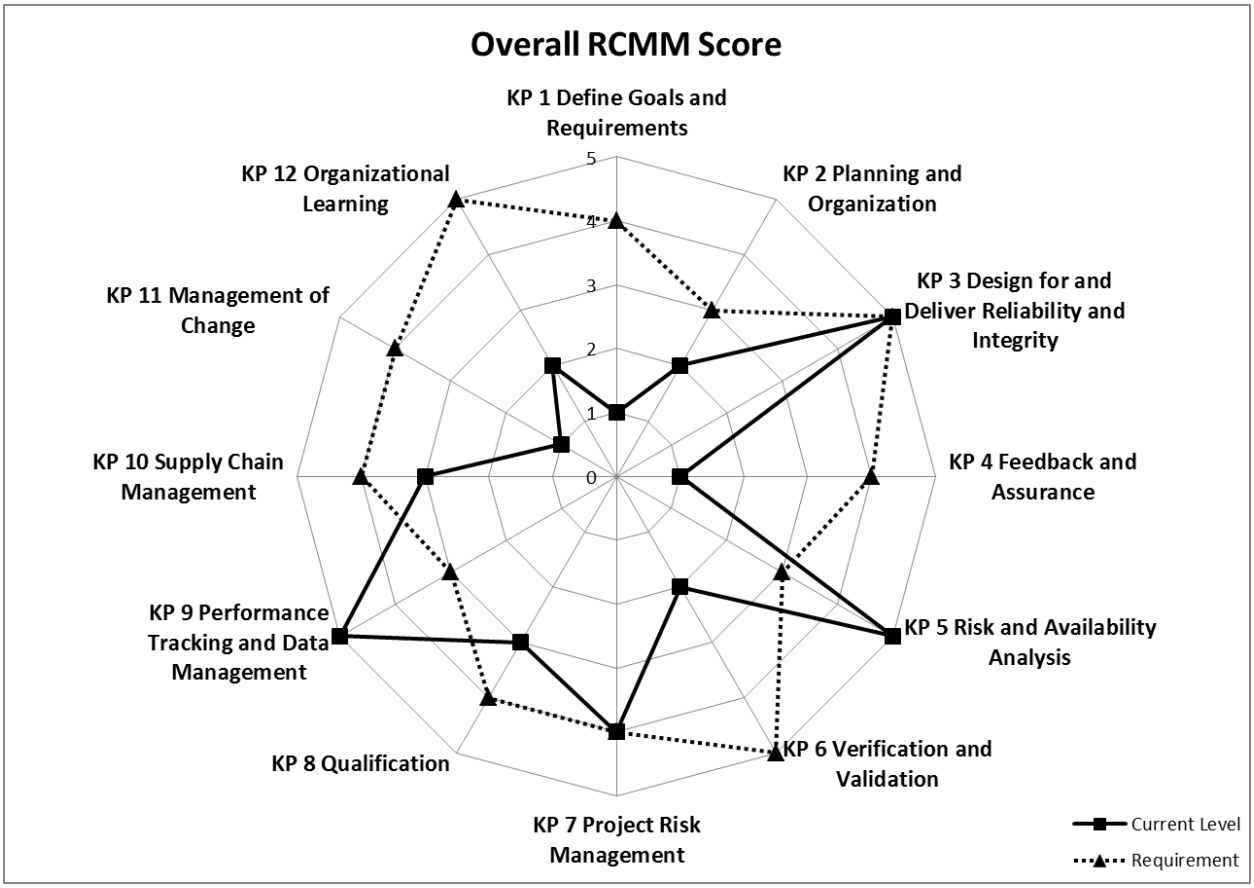


Figure B.7—Example Output from an RCMM Audit

For further details on capability maturity of organizations see References [22] and [23].

B.12.5 Additional Guidance

B.12.5.1 Obsolescence Management

Components, tooling, suppliers, processes, or knowledge that become obsolete during a project can introduce significant operational and financial risks to projects and the operator's business.

Operators are recommended to provide high-level guidance on the strategy to be adopted for the management of obsolescence and for the creation of obsolescence management plans addressing the prediction and prevention of obsolescence during design and MATIC stages as well as activities to resolve emergent obsolescence issues in operation.

The obsolescence management plan should be applied throughout the entire asset life cycle from concept selection and throughout operation to decommissioning. As a minimum the plan should include:

— obsolescence management objectives;

— obsolescence management strategies for managing obsolescence risks;

— obsolescence management organization, with:

  — details of the organization and individuals responsible for planned activities;

  — resources needed to ensure that planned activities can be undertaken and managed;

- identification of critical components;
- obsolescence risk assessments;
- means of managing the risks including:
  - design of products tolerant of component obsolescence (e.g. use of standard components in products or modularization strategy with defined standard interfaces);
  - identification of means for resolving obsolescence risk in operations;
  - CM to ensure design evolution due to obsolescence is managed in accordance with the product life cycle process and that it is sustainable;
- monitoring and communication plans to include:
  - product change/data notices, or life notices;
  - obsolescence status of critical components including impact on availability and mitigation costs;
  - new technology and system upgrades;
  - management of “commercial of the shelf” product;
  - the equipment stock level status.

B.12.5.2 Supplier Reliability and Integrity Specification in Contracts

Suppliers are crucial to the success of any asset development and operation and as such have a real opportunity to support the improvement of performance, integrity, and reliability. Simply seeking the lowest cost supplier may not deliver the greatest value to the project.

It is strongly recommended that reliability and integrity engineering is a specific part of the contractual agreement between the operator and the contractor/supplier.

The contracting strategy is an important tool for delivery of value to the project, especially if schemes to incentivize reliability and integrity improvement are adopted to provide a win-win solution for operators and contractors alike.

Supplier specification content may include but should not be limited to the following.

- Quantitative reliability and integrity goals and requirements at system, package, component, or process level.
- The means by which the supplier will provide assurance of meeting requirements.
- Minimum organizational capability and competencies required with regard to:
  - reliability and integrity data management;
  - quantitative reliability analysis;
  - qualification testing.

- Minimum requirements for undertaking reliability and integrity activities as part of the supplier's scope of supply. This may include requirements to undertake or participate in:
  - TRC assessments;
  - TRL assessments;
  - FMECA studies;
  - systems reliability analyses (e.g. using RBD, FTA, or ETA);
  - TRARs.
- Requirements to collate evidence of reliability and integrity activities undertaken together with achievements in an RIAD.
- Minimum requirements for internal procedures to address reliability and integrity KPs such as MOC, qualification testing as outlined in this RP.
- Process verification studies for manufacturing and quality control.
- Warranty data on installed systems or reliability calculations based on in house test data.

B.13 KP 11—Management of Change (MOC)

B.13.1 Objectives and Preparation for KP 11

During a project or operations there may be many instances where changes need to be made. Any changes (e.g. to scope, design, plan, or process in the project stage, or to procedures, remedial intervention, field upgrades, etc. in the operations stage) are likely to have significant consequences on the system RIM performance, especially following detailed design. Such changes should be risk assessed and evaluated against any assumptions that led to the original (pre-change) design, and any equipment, procedures, analyses, or models that are affected by or depend upon the change will need to be updated (see data management KP 9). A CM process should be established that maintains the consistency of a product's attributes with the requirements and product configuration data throughout the product's life cycle.

The objective of an MOC system is to ensure that any changes in the project (e.g. to scope, design, plan, process, etc.) or in operations (e.g. changes to procedures, remedial intervention, field upgrades, etc.) are consistent with the reliability, integrity, and technical risk management goals and requirements and that the change and impacts are fully assessed and managed.

B.13.2 Recommendation for Senior Management

- Define expectations and provide resources for the creation of a process for MOC.
- Define expectations and provide resources for the creation of guidance notes and good-practice documents for MOC that describe:
  - information systems to be used;
  - procedures to be used;
  - assessment procedures to be undertaken;
  - decision-making and acceptance criteria.
- Provide access to relevant training for MOC.

B.13.3 Recommendations for Project and Operations Management

— Ensure that agreed MOC protocols and procedures are applied in projects and operations.

— Create bridging documents between operator's, contractor's and supplier's MOC systems, as needed, to ensure consistency.

B.13.4 Process 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 to:

— monitor and identify when changes have occurred or are expected to occur;

— recognize when formal changes are required in relation to:

  — design improvements, revisions, upgrades;

  — changes in loading, installation, interface or operating requirements;

  — changes in material or welding properties, manufacturing tolerances;

— assess and evaluate risks introduced to the project/operations as a result of change;

— assess the impact that change may have on:

  — product or system reliability and integrity performance;

  — operability and maintainability of the installation.

It is then necessary to review the categorization of the component, package, or product in light of the changes that have been made.

B.13.5 Additional Guidance

Applicable risk assessment procedures for an MOC system include:

— FMECAs;

— risk reviews;

— HAZOPS and HAZID;

— design review and peer review processes.

MOC procedures should address the means of control and follow-up of necessary actions. These should:

— ensure that all affected parties are informed of the change and any associated actions are communicated and controlled including:

  — updates to all drawings and documentation;

  — revisions of analyses (engineering, reliability and integrity) and testing;

  — updates to the reliability and integrity plan and the RIAD;

— ensure that procedures are in place for monitoring and bench marking changes and follow-up actions.

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 or integrity are formally assessed, managed, documented, communicated, and approved through all the life cycle 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 asset life cycle.

B.14 KP 12—Organizational Learning

B.14.1 Objectives and Preparation for KP 12

The objective of KP 12 is to provide a common framework to capture organizational experiences over an asset's life cycle and communicate them back into the organization to enable teams in other parts of the organization to learn and benefit from these experiences.

B.14.2 Recommendation for Senior Management

- Define expectations and provide resources for the creation of a process for knowledge management and organizational learning that addresses:
  - procedures for capture and organizational absorption of important lessons;
    - created within a given organization/asset (e.g. during projects and operations);
    - created outside the organization by other organizations (e.g. research, publications, and conferences);
  - methods for storage and retrieval of lessons learned;
  - methods for dissemination of knowledge within the organization and down the supply chain;
  - methods and processes for exploitation of knowledge in new projects and operations;
- Provide resources to develop and manage lessons learned databases to ensure effective capture, storage, and dissemination of lessons.
- Define expectations and provide resources for the creation of guidance documents that describe:
  - procedures and methods for capturing and accessing lessons learned;
  - criteria for generating lessons learned data during projects and operations;
- Provide time and access to relevant training for project and operations teams in the practical use of lessons learned.

B.14.3 Recommendation for Project and Operations Management

- Project managers should ensure that
  - significant lessons are captured and documented at the end of each project stage;
  - important lessons are accessed and input to the project team at the start of each project stage;
- Operations managers should ensure that major system failures and operability or maintainability problems are captured as lessons learned and disseminated to enable other projects and operations to learn from the experiences.

B.14.4 Process Description

B.14.4.1 General

Each project is a mine of useful knowledge and experiences. The collection, review, and implementation of lessons learned from previous and current projects and operations 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 and operations.

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

— **Human Capital.** Knowledge of individuals in the organization.

— **Structural Capital.** Knowledge structured in databases and knowledge bases (lessons learned).

— **Customer Capital.** Knowledge of the company's value to customers.

B.14.5 Additional Guidance

B.14.5.1 Learning Competencies

B.14.5.1.1 General

There are four primary competencies for a learning organization:

— absorption of knowledge from the outside (lessons learned capture);

— generation of knowledge from within (lessons learned capture);

— diffusion and transmission of knowledge within the organization and down the supply chain (dissemination);

— exploitation of knowledge in projects.

Table B.18 provides some examples of instruments for learning.

B.14.5.1.2 Absorption and Generation (Lessons Learned Capture)

Lessons (concerning the successes and failures of the organization) should be captured on a formal basis at each life cycle stage and especially during operations.

These lessons provide valuable input to new projects and should be addressed and considered at every stage of the project and in operations as part of the risk, reliability, and integrity review activities including design reviews.

If this is carried out as part of a formal system, then it is expected to be more effective and should ensure that it is carried out and at the right time.

Lessons relating to the achievement of reliability and integrity may be very diverse but should as a minimum address:

— equipment (design, manufacture, installation, and operational difficulties or successes);

— procedures (clarity, implementation, and approval);

— project management (schedules, budgets, risks).

B.14.5.1.3 Absorption of Knowledge from the Outside

Lessons can be gathered from a range of sources including technical experts, project best practices, historical failure and maintenance data, engineering test and inspection reports, industry networks and communities of practice, conferences, research publications, supplier bulletins, etc. (see Table B.18).

Table B.18—Typical Instruments for Organizational 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
Contractor's R&D		Action learning	

B.14.5.1.4 Generation of Knowledge from Within

Every member of the relevant team should be responsible for ensuring that they have each identified and captured all lessons pertinent to their role and area of responsibility within the project and operations.

An important tool in lessons learned capture is root cause analysis of failures and successes (see B.7). This tool facilitates companies in understanding the technical root causes of both.

Important lessons may also be found in FRACAS databases.

B.14.5.1.5 Project Lessons Learned Review

The lessons learned review may be performed separately or facilitated as part of a project risk review process.

The review should aim to identify operational successes and failures and document historical evidence of these events during each individual life cycle stage. The review is best carried out prior to the commencement of the TRC, so that experience from previous projects can be reviewed.

In operations, the lessons learned review is a continual process implemented as significant events occur or operational conditions change.

During this task, all relevant data from previous projects and operations should be elicited from appropriate databanks or knowledge management systems. The lessons learned usually cover the whole life of the asset from strategic thinking and decision-making, through project execution, operations, and decommissioning. It is essential that these lessons explicitly address any issues that impact the ability to achieve reliability and integrity, from both good and bad practice.

B.14.5.2 Dissemination of Knowledge

For knowledge to be useful, it must be disseminated to engineers and managers in the project, operations, or supply chain 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 stage gate reviews and operations reviews;

— providing engineers with 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.14.5.3 Exploitation of Knowledge in Projects

The tracking, analysis, dissemination, and storage of data have most value when the information can be converted into organizational knowledge that adds value to the business and its customers.

This may be through improved products and services for delivery of reliability and integrity. 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.

The knowledge generated should be reviewed by the design and operations team and their managers at every stage of the asset life cycle to ensure that best practice is adopted or best value decisions are made. This may entail R&D to develop prototypes or new products, services, and procedures.

Lessons learned input early in design (e.g. conceptual design or at start of a new project stage) is important to ensure exploitation of knowledge is instigated from the beginning of the asset’s life cycle.

Annex C
(informative)

Risk-based Scope of Work for Reliability, Integrity, and Technical Risk Management

C.1 General

This annex provides details of recommended RIM activities to be included in the required scope of work at each asset life cycle stage based on the identified level of technical risk.

This RP recommends the use of TRC (see Annex A) to categorize the level of technical risk.

In addition to the risk-based activities recommended in this annex, the scope of work should include the generic activities that should be implemented at each life cycle stage at the appropriate level of detail (project level, system level, package level, etc.) for all technical risk categories.

— **Review of Lessons Learned.** Collate and review lessons learned for comparable subsea developments/operations and required technologies to ensure relevant lessons are addressed in technical risk assessments, goals and requirements, and reliability, integrity and risk management activities (see 5.4.2).

— **Identification of Technical Risk and Uncertainty.** Assess at a high level, the technical risks relative to previous experience with similar designs to identify aspects/items with high technical uncertainty (see 5.4.3 and Annex A).

— **Generation of Goals, Requirements, and Strategy.** Identify goals and requirements together with a strategy for how these are to be achieved (see 5.4.4, 5.4.5, and B.3).

— **Identification of Scope of Work.** Define a required scope of work that can be accomplished within the project stage/operations integrity management campaign (see 5.4.6 and this Annex C).

— **Creation of Implementation Plans for Required Scope of Work.** Create a more detailed plan, aligned with the wider project/operations schedule, identifying how the activities identified in the scope of work are to be accomplished (see 5.5 and B.4)**.**

— **Implement Planned Scope of Work.** Implement planned activities to provide assurance that the identified technical risks have been addressed sufficiently to move to next project stage/in operations (see 5.6).

— **Evaluate Actions Against Goals and Requirements.** Assess the project technical risk level and evaluate against risk acceptance criteria (see 5.7).

— **Collation of Lessons Learned.** Report any lessons learned that could be of benefit to future projects in relation to project execution, novel technology, and new lessons learned gathered from operating assets (see 5.8.2).

— **Provision of Reliability and Integrity Assurance.** Collate all information generated from the scope of work into the RIAD (see **Error! Reference source not found.** and B.6).

The recommended scope of work in the tables below is generic based on the life cycle stage and risk category and is for guidance only. Additional life-cycle-stage-specific guidance is also provided for some generic activities. All risks should have an associated scope of work to address them.

C.2 Feasibility Stage

C.2.1 General

Reliability, integrity, and technical risk management during feasibility is at the **project level** and contributes to the identification of viable concepts and approaches to economically exploit the field**.**

Overall reliability and integrity effort is expected to be relatively low or very low during this initial project stage (see A.4).

C.2.2 Additional Stage-specific Generic Activity Guidance

Additional feasibility-stage-specific guidance for generic activities includes the following.

- **Lessons Learned.** Address in technical risk assessments and goals and requirements for project.
- **Goals and Requirements.** Document as simple statements of what the project has to achieve in terms of production availability and integrity performance.
- **Strategy.** Identify how the overall goals and requirements for the asset are to be achieved, e.g. through:
  - application of field proven equipment;
  - deployment of new technology;
  - procedural controls to minimize the risk of human error;
  - a high reliability rather than maintainability strategy.
- **Scope of Work.** Include accountability to drive processes and activities throughout the asset life cycle. Establish that the project is technically and economically feasible and consider:
  - system availability expectations and their consistency with financial goals and available technology/processes;
  - additional risk-based activities (see C.2.3).
- **Plan.** This may be a simple table scheduling and resourcing the scope of work, with relevant milestones, such that the generated output can support decision-making.
- **RIAD.** This will typically include conclusions regarding the feasible of exploiting a field (or product if a product development project) and whether standard or novel technology would be required for exploitation. It may also include requirements or recommendations to demonstrate a minimum level of reliability or availability.

C.2.3 Additional Stage-specific Risk-based Scope of Work

C.2.3.1 Category A (Very High Risk) and B (High Risk) Projects

In addition to the generic activities:

- for each area of technical uncertainty, determine the qualification status (TRL assessment; see B.10) across all potential suppliers to identify the qualification effort that will be required during the project for deployment of the technology (at this stage, this should be at the system level, but may focus on key equipment that is the source of the uncertainty);

— contact suppliers of equipment to establish the effort in terms of cost and schedule to develop a qualified system to enable realistic predictions of overall project costs and schedule to be made. Build this into the preliminary project schedule with enough float to account for the accuracy of the information;

NOTE In some instances, the qualification schedule may determine the project schedule.

— where uncertainty exists over the project organization, prepare a preliminary project execution plan to address the potential risk from this. This may involve changing the project team location to be able to better access a company knowledge base, or involve relocating key experience to the remote project location.

C.2.3.2 Category C (Medium Risk) and D (Low Risk) Projects

Generic activities may suffice.

C.3 Concept Selection

C.3.1 General

Reliability, integrity, and technical risk management during concept selection is at the overall subsea **system level** and contributes to the selection of the **best value** concept for the system design and operations.

For Category C and D concepts, the overall reliability and integrity effort is expected to be relatively low during this project stage (see A.4).

The number of concepts to be addressed should be reduced to a manageable number before application of the recommendations of this RP.

C.3.2 Additional Stage-specific Generic Activity Guidance

Additional concept-selection stage-specific guidance for generic activities includes the following.

— **Lessons Learned.** Apply for each concept and address in RIM activities for the concept.

— **Identify Technical Risk.** Carry out high-level TRC for each concept to identify any concept aspects or constituent packages with high technical uncertainty:

  — some risk factors of the TRC assessment (e.g. those dependent on geographical location) will result in the same risk level being awarded for each concept for that factor;

  — other risk factors, in particular reliability, technology, and architecture, will be highly dependent on the concept itself and the novelty/uncertainty of the technology required for that concept.

— **Goals and Requirements.** Translate asset goals and requirements into specific concept reliability and integrity goals and requirements, recognizing the novelty of the technology required for the concept and operational process risks related to the technology (see B.3), including:

  — production availability targets or requirements;

  — containment and isolation requirements;

  — technology and readiness requirements for each concept;

  — risk acceptance criteria (if not previously defined). Agree risk acceptance criteria with the operations team.

- **Strategy.** Identify how each concept will achieve the asset goals and requirements, e.g. through:
  - identification of appropriate system-level isolations to meet integrity requirements;
  - system redundancy to achieve availability goals/requirements;
  - high-level review of integrity manageability (e.g. can the system be pigged);
  - procedural controls on operational processes to achieve low levels of human error.
- **Scope of Work.** Establish technical and commercial value for each concept and consider:
  - risk-based activities identified in C.3.3;
  - reliability and integrity goals and requirements for the constituent equipment packages derived from the overall concept goals and requirements (allocated from the system RAM/reliability analyses);
  - ability of the system concepts to meet the isolation and containment requirements (e.g. by system reliability analysis/fault tree analysis/bowtie diagrams);
  - ability of testing, manufacturing, and operational processes to meet reliability and availability goals and requirements (e.g. HAZOP, P-FMECA);
  - plan for obsolescence management.
- **Plan.** This may be a simple table scheduling and resourcing the scope of work, with relevant milestones, such that the generated output can influence concept selection decisions (see B.4). Split the plan by system concept with high-risk concepts given more effort than low-risk ones.
- **Implement.** For concepts where identified technical risks cannot be sufficiently addressed or if new information reveals that the concept is no longer technically or commercially viable, these may be dropped before the completion of the planned activities.
- **Evaluate.** Revisit the technical risk level of each concept with involvement from the operations team and evaluate against risk acceptance criteria. For each concept:
  - review the system availability predictions to confirm the production goals and requirements can be achieved;
  - review the system architecture to confirm there is sufficient isolation capability, and adequate provision for inspection and monitoring, to meet integrity requirements and risk acceptance criteria;
  - review the technology qualification status to confirm the current level of technical uncertainty, and hence technical risk to project delivery, is acceptable to proceed to the next project stage;
  - review the technology qualification plan to confirm that the required qualification activities can be achieved within the project schedule and budget requirements.
- **RIAD.** Identify the option that best satisfies the concept selection criteria and demonstrates that:
  - the reliability and integrity goals and requirements can be met by the concept;
  - the recommended option provides the greatest opportunity to meet the project’s financial objectives;
  - the technical risks identified for the recommended concept can be managed, including necessary qualification activities, within the project schedule and budget.

C.3.3 Additional Stage-specific Risk-based Scope of Work

C.3.3.1 Category A (Very High Risk) and B (High Risk) Concepts

In addition to the generic activities:

— estimate the qualification status (TRL assessment; see B.10) of the concept and establish the effort in terms of cost and schedule to qualify the concept technology;

— review the concept against the subsea system production and integrity goals and requirements to assess the concept's ability to deliver this (or better) performance (e.g. by simple RAM analysis to predict production availability);

— provide a relative comparison of technical risks with other competing concepts (e.g. by a system-level functional FMECA; see B.7) to identify integrity threats of new technology;

— 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. Include the cost and benefit of any improvements in the overall commercial comparison of options;

NOTE 1 Improved designs may also need to be qualified (see first item).

NOTE 2 Reliability improvements may require significant qualification or re-qualification effort.

— for any concept where uncertainty exists over the project organization and its supply chain, develop a concept-specific project execution plan to address the potential risk from this. Include any financial impact in the overall commercial comparison of options;

— complete a preliminary project schedule and value analysis for the concept to compare through life cost and ensure that the concept selected is of optimum value. Include both the qualification status of the concept and the costs of developing it for the project together with the potential reliability and integrity benefits.

C.3.3.2 Category C (Medium Risk) and D (Low Risk) Concepts

In addition to the generic activities:

— confirm the system concept can achieve the project production and integrity goals and requirements with reference to previous similar systems (e.g. updated RAM analysis). Actual relevant performance data are preferred to generic historical data;

— complete a preliminary project schedule and through life cost/value for the concept (to provide like for like comparison against A and B concepts). Actual costs are preferred to previous estimates.

C.4 FEED

C.4.1 General

Reliability, integrity, and technical risk management during FEED is at the subsea **package (or subsystem) level** (e.g. tree system, control system, etc.) to confirm functionality and performance can be delivered at the expected cost.

Packages should ideally be identified so that each will eventually be supplied by a single supplier.

C.4.2 Additional Stage-specific Generic Activity Guidance

Additional FEED-stage-specific guidance for generic activities includes the following.

— **Lessons Learned.** Apply for each package and address in RIM activities for the package.

— **Identify Technical Risk.** Carry out high-level TRC for each equipment package:

  — the risk level for the reliability factor should reflect the system reliability performance assumptions used in the system modeling as part of concept selection;

  — the risk level for the technology and architecture factors should reflect any changes required to the package technology and architecture to meet the package reliability and integrity goals and requirements in the intended operating environment.

— **Goals and Requirements.** Translate the reliability and integrity characteristics used as the basis for concept selection into detailed goals and requirements for each package (see B.3).

— **Strategy.** Identify how the package will achieve its reliability and integrity goals and requirements by:

  — further developing the package-specific reliability and integrity goals and requirements and allocating to equipment items within the package;

  — identifying any equipment redundancy to achieve integrity requirements, package reliability goals/requirements, or availability goals/requirements;

  — identifying any inherent reliability or integrity improvements within the package equipment to achieve package integrity or package reliability goals/requirements;

  — identifying any required package isolations to meet integrity and intervention requirements;

  — developing baseline integrity management tasks, responsibilities, and requirements with input from the operations team;

  — identifying reliability and integrity risk acceptance criteria;

  — identifying procedural controls on operational processes to achieve low levels of human error.

— **Scope of Work (System Level).** System-level activities include:

  — a review and update of the production availability models for the subsea system as a whole, integrating the package detail, to confirm that overall production availability performance will meet expectations;

  — management of package interfaces from a reliability and integrity perspective;

  — identification of any key vessel or sparing requirements to support achievement of production availability goals and requirements;

  — identification of any long lead items to enable prioritization of individual and joint reliability, integrity, and risk management effort between operator and supplier such that activities are completed in line with the project timeline (see Figure C.1).

— **Scope of Work (Package Level).** The deliverable for each package scope of work should be detailed package goals and requirements to be included in the package supplier requirements document developed during FEED. These should be specified in terms of:

  — functional requirements for equipment including all integrity requirements;

  — reliability goals and requirements for the package;

  — integrity manageability requirements for the package;

  — additional risk-based activities defined in C.4.3;

  — scope of reliability analysis to be carried out in detailed engineering, if appropriate.

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

— **Plan.** Split by system, package, and package subsystems 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. Where any activity is to be outsourced (e.g. complex reliability and integrity modeling), a more detailed plan may be required. Some level of independent verification (e.g. third-party review or organized peer review) is appropriate at this life cycle stage and should be included in the plan.

— **Evaluate (Package).** For each package:

  — review the package architecture to confirm there is sufficient isolation capability to meet integrity requirements and meet risk acceptance criteria;

  — review the technical risks for the package to confirm appropriate integrity manageability has been included in the design;

  — review the reliability capability of potential contractors and suppliers against acceptance criteria;

  — confirm testing, manufacturing, and operational processes meet reliability and availability goals and requirements.

— **Evaluate (System).** For the subsea system as a whole:

  — review the final system architecture to confirm there is sufficient isolation capability to meet integrity requirements and risk acceptance criteria;

  — confirm package interfaces risks have been addressed and meet acceptance criteria;

  — confirm key vessel or sparing requirements have been addressed and meet acceptance criteria;

  — confirm operational processes meet reliability and availability goals and requirements.

— **RIAD.** Specifically demonstrate that:

  — reliability, integrity, and integrity management goals and requirements placed on suppliers of equipment have been identified and are consistent with overall subsea system design reliability and integrity goals and requirements and the project’s overall financial objectives;

  — a through life cost-benefit analysis has been carried out and all assumptions recorded.

C.4.3 Additional Stage-specific Risk-based Scope of Work

C.4.3.1 Category A (Very High Risk) and B (High Risk) Packages

In addition to the generic activities:

— confirm the qualification status (TRL assessment; see B.10) of the package and develop the test program to be carried out by suppliers of that package, to estimate remaining effort required in terms of cost and schedule;

— carry out a package-level reliability/availability analysis (package system RBD/FTA/ETA; see B.7):

  — to confirm that the package system availability performance is sufficient for the overall subsea system to meet production availability goals and requirements;

  — to assess the potential for failure to isolate wells or key pressure containing components;

  — to assess the potential for common cause failures;

  — to identify the intervention decision logic in the event of failure of equipment that forms part of the package (e.g. valve failure);

— where new technology within the package means there is no useful performance data, use a package-level functional FMECA (see B.7) to understand potential failure modes and predict reliability performance. This is also useful in developing a qualification test program allowing tests to match potential failure modes (to confirm they have been designed out or mitigated) (see B.10);

— consider the need for package reliability and maintainability improvements by investigating the through field life cost/benefits of different package configuration options, any relevant project lessons learned, including those from relevant operations. Assess the benefit of different integrity management and maintenance strategies (e.g. RCM);

— identify integrity management requirements (HAZOP, HAZID, bowtie) for the package equipment in conjunction with the operations team to ensure appropriate monitoring and inspection capability is included in the package specifications;

— after any package improvements are incorporated, update the package reliability and availability analyses to identify package RAM expectations (rationalized by historical data) to be included in package functional specifications to be sent to suppliers;

NOTE The requirement in the specification should be for this reliability/availability to be demonstrated by the supplier. Suppliers that do not have reliability/availability analysis capability should be asked to provide the necessary data (see B.11) so others can undertake analysis (this may be part of a later detailed system RAM analysis).

— consider the reliability capability of potential contractors and suppliers to effectively assess and deliver against the reliability requirements as part of the supplier selection process along with the standard selection criteria (see B.12);

— for any package where uncertainty exists over the project organization and its supply chain, develop a package-specific project execution plan to address this risk. Include any financial/schedule impact in the overall level project schedule and through life cost. Add any requirements identified for equipment suppliers to the project execution requirements specification for tendering (e.g. percent local supply, skills requirements for local supplier, etc.);

— complete a subassembly-level project schedule and through life cost for the package that reflects the reliability and integrity effort identified through the work above (and may account for different supplier's equipment). Identify in the project execution plan or similar how the full scope of work will be managed.

C.4.3.2 Category C (Medium Risk) and D (Low Risk) Packages

In addition to the generic activities:

— Review the package against the reference systems it is based on to confirm that performance data from the reference system is still relevant. Consider any relevant lessons learned, including those from relevant operations. If additional changes are required, the activities for A and B packages above apply. Actual relevant performance data are preferred to generic historical data.

— Complete a subassembly-level project schedule and through life cost for the package that reflects the reliability and integrity effort identified through the work above. Identify in the project execution plan or similar how the full scope of work will be managed.

C.5 Detailed Design

C.5.1 General

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

During detailed design, activities are implemented both by the operator and subsea system project team and by the supplier; see Figure C.1.

Responsibility for meeting reliability and integrity goals and requirements transfers to equipment suppliers as they undertake detailed engineering design ahead of manufacture.

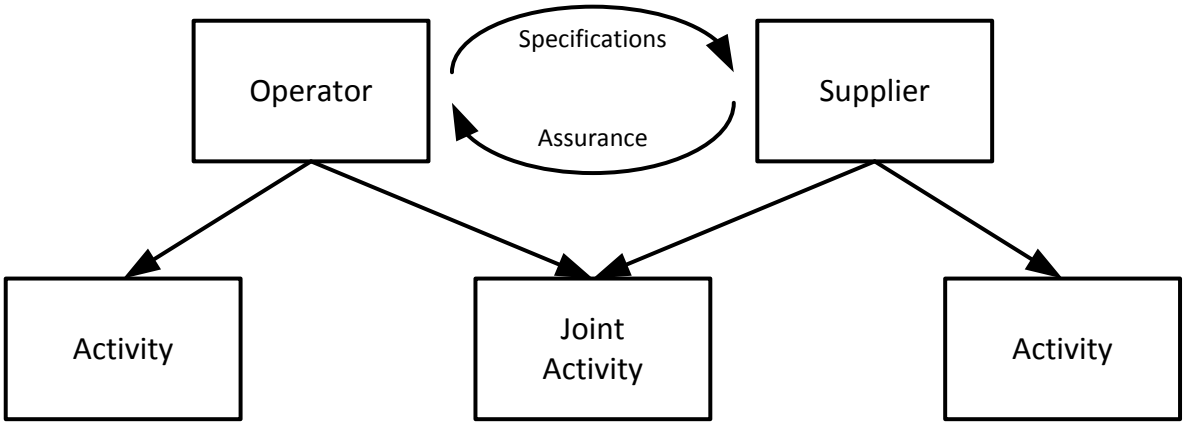


Figure C.1—Typical Relationship Between the Operator and Supplier with Respect to Activities

NOTE Detailed design often involves a major transition of project execution responsibility from the operator project development team 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 reliability and integrity activities performed during the FEED stage of the project and becomes an important reliability and integrity specification input to the package supplier.

In parallel with detailed design activities, suppliers and contractors should also be implementing risk assessment activities associated with the MATIC stages (see C.6). In addition, work should begin on the development of an ITMM plan (see Annex D) for integrity management in operations. Requirements for process controls to minimize human error should flow down from the operator to the supplier.

C.5.2 Additional Stage-specific Generic Activity Guidance

Additional stage-specific guidance for generic activities includes the following.

- **Lessons Learned.** Include lessons learned related to management of the supply chain and operations.
- **Identify Technical Risk.** The package design team (supplier or subcontractor) should carry out a TRC assessment for each component of the package:
  - the risk level should reflect any changes in the sub-supply chain for constituent parts of the component (e.g. valve body, seat, or seal);
  - sub-suppliers may need to participate in assessments;
  - the end user (operator) of each component should either participate in the assessment or validate the supplier assessment.
- **Goals and Requirements.** Suppliers may have their own additional goals and requirements for the project execution. The operator and the supplier should agree upon the goals and requirements for the package and how achievement is to be demonstrated by the supplier (e.g. through process controls and setting agreed metrics):
  - the reliability, integrity, and integrity manageability goals and requirements for each package and its key assemblies/subassemblies identified in the detailed design specification should be allocated to subassemblies/components and constituent parts within the package (see B.3);
  - allocation of package goals and requirements to components should make use of reliability/availability system modeling tools (see C.5.3 and B.7);
  - if the tool demonstrates that the package system architecture delivers the required availability/reliability, then the component reliability and maintainability input data [e.g. mean time to failure (MTTF)/MTTR] become the component requirements;
  - if the tool demonstrates that the package architecture cannot meet the availability/reliability specification, then some component reliabilities will need to be stretched beyond that which has been historically achieved, or the system architecture will need to be reconfigured to achieve the specifications;
  - a description of a complete reliability allocation procedure is beyond the scope of this RP and reliability specialists should be consulted as needed to support the allocation process;
  - consideration should be given to incorporating monitoring points that capture real data of applied stresses and critical parameters during operations. This will be in accordance with the ITMM plan (see Annex D).
- **Strategy.** The strategy for each equipment component of the package should be based on the strategy for the package e.g. through:
  - application of redundancy;
  - management of obsolescence;
  - use of bought in items;
  - use of high specification parts;
  - redesign to improve inherent reliability;
  - procedural controls on operational processes to achieve low levels of human error.

- **Scope of Work (System).** Define a scope of work for the subsea system as a whole. Activities at a subsea system level would normally be undertaken and led by the operator subsea project team (including input from operations) and include:
  - a review and update of the production availability modeling for the subsea system as a whole, integrating the package and component detail, to confirm that overall production availability performance can meet or exceed expectations;
  - requirements for management of package interfaces (from a reliability, integrity, integrity management, obsolescence, and qualification perspective);
  - review of installation and intervention requirements (vessel or sparing) to support achievement of production availability goals and requirements;
  - use of independent expert reviews of the design;
  - requirements for auditing of supplier reliability capability for high-risk items.
- **Scope of Work (Package).** Define a scope of work for each package subassembly/component. The package scope of work normally implemented by the supplier should be split by subassemblies/components and consider:
  - risk-based activities as defined in C.5.3;
  - application of component-level system reliability/availability analysis to confirm overall package availability performance will meet expectations with the actual components selected;
  - use of peer reviews/lessons learned reviews including those from relevant operations and human reliability experts to add experienced input to the design.
- **Plan.** A detailed plan should be developed by the supplier with appropriate milestones. This may cover one or several packages in response to the reliability and integrity specification and agreed by the end user (operator) prior to execution (see B.4). Suppliers should consider incorporating this plan into their project execution plan, to ensure that the reliability and integrity activities link to and influence other project execution activities. The plan should specify how each activity will be validated and verified, i.e. 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.
- **Implement.** Whilst the component activities are implemented by the supplier, subsea system integration activities should be led by the operator subsea project team with input from suppliers of packages that interface with each other. It is important that the activities are implemented at the right time to support design decisions; this may include working with the sub-supply chain.
- **Evaluate (System).** For the subsea system as a whole:
  - review the final system architecture to confirm there have been no changes that impact isolation capability and ability to meet integrity requirements and risk acceptance criteria;
  - confirm package interface risks have been addressed and meet risk acceptance criteria;
  - confirm installation/intervention requirements (vessel or sparing) and operational requirements have been addressed and meet risk acceptance criteria.

— **Evaluate (Package).** For each subassembly/component:

  — review the reliability/availability predictions to confirm capability to meet the package availability and integrity goals and requirements and meet risk acceptance criteria;

  — review the technical risks for the component to confirm that appropriate integrity manageability has been included in the design.

— **Feedback.** Suppliers should collate package activities into an RIAD for the package for subsequent integration into the RIAD for the subsea asset as a whole. The subsea asset RIAD should also be updated with project-level activities (e.g. subsea system production availability analysis).

C.5.3 Additional Stage-specific Risk-based Scope of Work—Detailed Design—Scope of Work

C.5.3.1 Category A (Very High Risk) Components/Subassemblies

In addition to the generic activities:

— undertake a detailed component FMECA to identify potential failure modes and define clear actions/mitigations to improve design reliability and integrity (see B.7);

— identify additional mitigations/monitoring/control to be adopted as part of integrity management in operations (i.e. expand the FMECA results to develop an appropriate integrity management strategy where inspection and monitoring frequency is based on a risk of failure assessment) to ensure that any residual risks are deemed acceptable;

— undertake a detailed assessment of the subassembly/component's qualification status (e.g. TRL) and, for any unqualified items, confirm that a defined test program has been developed that meets all project functional integrity/integrity management and reliability requirements within the project delivery schedule (see B.10);

— implement the qualification program as appropriate to enable the required qualification status to be achieved at the right time in the project;

— on completion of the subassembly design, undertake a subassembly system reliability/availability analysis (or extend earlier package analysis) to confirm that performance at the subassembly level will achieve the high-level system availability goals (see B.7);

  NOTE 1 The reliability/availability model needs to reflect actual components (including constituent parts) to be used, so results can be interpreted by component (and weak links identified). The reliability/availability analysis may also be used to inform sparing, intervention and maintenance strategies.

  NOTE 2 If the supplier has been given package/assembly availability as a specification to be met, a tool for modeling package system availability will be more appropriate than a production availability tool. If the availability goal is in the form of a reliability target to be achieved, then a system reliability tool (e.g. RBD, FTA, or ETA) may be used. Application of the tool is typically at a level for which historical and acceptable data are available.

— where reliability or integrity achievement depends on the use of redundancy, CCFA (see B.7, Table B.9, and Table B.10) should be undertaken to ensure that single failure (common deficiency) does not undermine the assumed reliability or integrity;

— in addition to any project design reviews, invite external experts (independent of the project and the supplier) to review and challenge the design and its assumptions ahead of design freeze for manufacture;

— for any component where uncertainty exists over design team experience, consider altering the team or increasing peer reviews to add experienced input to the design;

— audit the supplier reliability capability to verify the competency of the company to undertake the work.

C.5.3.2 Category B (High Risk) Components/Subassemblies

In addition to the generic activities:

— modify/update the original detailed component FMECA, from previous application of the original (parent) component, to take account of the major modifications made and identify all new potential failure modes that could impact the design reliability and integrity (see B.7);

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;

— identify any additional mitigations/monitoring/control to be adopted in integrity management in operations as part of the FMECA review to ensure that any residual risks are deemed acceptable;

— undertake a detailed assessment of the subassembly/component's qualification status (TRL) and, for any (unqualified) modified items, confirm that a defined test program has been developed that meets all project functional integrity/integrity management and reliability requirements within the project delivery schedule (see B.10);

— implement the qualification program as appropriate to enable the required qualification status to be achieved at the right time in the project;

— on completion of the subassembly design, undertake a subassembly system reliability/availability analysis (or extend earlier package analysis) to confirm performance at the subassembly level will achieve the high-level system availability goals (see B.7);

NOTE 1 The reliability/availability model needs to reflect actual components (including constituent parts) to be used, so results can be interpreted by component (and weak links identified). The reliability/availability analysis may also be used to inform sparing, intervention, and maintenance strategies;

NOTE 2 If the supplier has been given package/assembly availability as a specification to be met, a tool for modeling package system availability will be more appropriate than a production availability tool. If the availability goal is in the form of a reliability target to be achieved, then a system reliability tool (e.g. RBD, FTA, or ETA) may be used. Application of the tool is typically at a level for which historical and acceptable data are available;

— where reliability or integrity achievement depends on the use of redundancy, CCFA should be undertaken to ensure that a single failure mode does not undermine the assumed reliability or integrity;

— in addition to any project design reviews, invite external experts (independent of the project and the supplier), including relevant operational expertise, to review and challenge the component design and its assumptions ahead of design freeze for manufacture;

— 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;

— review the supplier reliability capability to verify that the company has the reliability and integrity capability to manage a project requiring them to achieve the stated reliability of the component.

C.5.3.3 Category C (Medium Risk) Components/Subassemblies

In addition to the generic activities:

— undertake a detailed assessment of the component's qualification status (e.g. TRL) to confirm that notionally qualified equipment is backed up by the test record that the test is to the same standard as the project requires and the tested component is the same unit as that proposed for the project;

— review the component against previous reference applications, of the original (parent) component it is based on, to confirm that performance data from each reference application is still relevant. If not, the bullets above (TRC B) apply. Actual relevant performance data are preferred to reliability/availability analysis predictions;

— review the subassembly/component interfaces to check for any changes that need to be addressed;

— verify that the detailed original (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;

— review the FMECA to identify if any additional mitigation/monitoring/control needs to be adopted as part of integrity management in operations to ensure residual risks are within risk acceptance criteria;

— in addition to any project design reviews, invite external experts (independent to the project/supplier), including relevant operational expertise, to review the overall system design ahead of design freeze for manufacture.

C.5.3.4 Category D (Low Risk) Components/Subassemblies

In addition to the generic activities:

— when all detailed 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).

C.6 MATIC

C.6.1 General

Reliability, integrity, and technical risk management during MATIC is at a **procedural** level but also addresses equipment, handling, and tools to be used as part of implementing the procedure.

During the MATIC stages, the focus moves from designing in reliability and integrity to ensuring that the designed-in reliability is realized through adequate QC/QA procedures.

During SIT and other system function testing, installation, and commissioning, system interfaces should be reviewed and addressed.

During the MATIC stages, reliability and integrity risk management activities are implemented by both the operator subsea system project team and by the supplier/contractor (Figure C.1), with some activities undertaken jointly.

The MATIC activities should be initiated with the supplier and installation contractor at an early stage in detailed design, well in advance of manufacture, and are integral to development of appropriate procedures for the MATIC stages.

Detailed procedures should be developed for each MATIC stage to ensure that all equipment is manufactured, assembled, delivered, installed, and commissioned correctly and all loads/environments that the equipment is exposed to during each MATIC stage are within its acceptable limits; this includes transit and storage.

The supplier/installer are responsible for demonstrating that all procedural requirements for the MATIC stages have been captured (some of which may be output from the design and human reliability analyses) and met.

In parallel with the MATIC activities, the ITMM plan for integrity management in operations is developed (see C.7 and Annex D).

C.6.2 Additional Stage-specific Generic Activity Guidance

Additional MATIC-stage-specific guidance for generic activities includes the following.

- **Lessons Learned.** Include lessons learned for each MATIC procedure and associated equipment/tooling.
- **Identify Technical Risk.** The package design team (supplier or contractor) should carry out a TRC assessment for each procedure (manufacture, assembly, etc.) and associated equipment/tooling:
  - the assessment should cover the different stages of the procedure;
  - a key aspect of the assessment is to identify the level of technical risk from the procedure to the reliability and integrity of the subsea system equipment being deployed;
  - the risk level should reflect any changes/novelty in the procedure or in the equipment/tooling to be used in applying the procedure (e.g. installation equipment);
  - for some procedures, the review team may need to include the project package delivery team, the equipment supplier/sub-supplier, the installation contractor, and operations team;
  - the end user (operator) of each subassembly/component should either participate in the assessment or validate the supplier/contractor assessment.
- **Goals and Requirements.** In addition to project availability and integrity goals and requirements, specific MATIC goals and requirements should be developed such that the procedures and equipment/tooling used in this stage of the life cycle will not compromise the reliability or integrity of the subsea system equipment being supplied and installed (see B.3).
  - **Manufacture and Assembly.**
    - to avoid the introduction of manufacturing defects and manufacturing/assembly errors;
    - to check for possible obsolescence of bought-in items during expected field life.
  - **Testing (Pre-installation).**
    - to avoid damage to equipment being tested (e.g. overloading);
    - to provide evidence to demonstrate function, performance, reliability, and integrity;
    - to reveal any latent defects (e.g. cracks, nicks in O-rings or leads) or incorrect assembly (e.g. substitution of incorrect or out of spec parts);
    - to confirm emergency response plans are effective;
    - to provide baseline data for comparison when testing during operations (as part of RIM).
  - **Installation and Commissioning.**
    - to prevent damage during installation such that reliability and integrity is compromised;
    - to prevent overloading (e.g. shock loads, dynamic loads, static loads);
    - to prevent delays to field start-up that could impact on meeting production availability requirements or cause unforeseen degradation of equipment;
    - to provide baseline data for comparison when testing during operations (as part of RIM).

- **Strategy.** At this stage the strategy has been set. The focus now shifts toward how to deliver on the pre-specified strategy.

- **Scope of Work.** A specific scope of work should be developed for each of the MATIC stages for each equipment package covering each of the procedures such that that the procedure receives inputs and reviews appropriate to the level of risk and that an appropriate level of verification is in place during implementation of the procedure.

  - Development of MATIC procedures should include verification that all integrity management activities can be performed as planned.

  - The scope of work should consider the risk-based activities identified in C.6.3.

  - The technical risks and hazards associated with each MATIC procedure should be assessed using appropriate risk assessment tools.

  - **Manufacture and assembly** scope of work should be aimed at**:**

    - reducing the risk of introducing defects or assembly errors that may lead to reduced reliability and integrity;

    - preventing damage, overloading, shock loading, or degradation during transit and storage between locations;

    - checking for components and parts that may become obsolete during the asset life cycle;

    - ensuring that vendors have the capability to deliver the inherent reliability and integrity of equipment within their scope of work (e.g. through an audit).

  - **Testing** scope of work should be aimed at providing assurance that:

    - the designed-in reliability and integrity have been achieved and have not been compromised by manufacture and assembly;

    - the test itself does not compromise reliability and integrity;

    - any subsea system equipment modifications to facilitate testing are restored to the required post-test configuration on completion of testing. For example, temporary hydraulic hoses that may need to be installed for testing but must be replaced by subsea hoses before installation;

    - processes and procedures for installation, commissioning, and decommissioning do not compromise reliability and integrity.

  - **Installation and commissioning** scope of work should be aimed at:

    - reducing the threat of introducing risks to reliability and integrity (e.g. from damage, overloading, incorrect or prolonged storage);

    - preventing of delays during installation and commissioning.

  - **Commissioning and handover** poses high risk to reliability and integrity achievement as inconsistencies between drawings and installed hardware and practical problems with procedures become evident to the commissioning and operations teams. It is therefore recommended to:

    - identify any unexpected changes to components, systems, or procedures that impact on reliability and integrity performance during commissioning;

- develop plans to update reliability and integrity assessments and models prior to, or early, during operation phase such as design FMECAs, IM-FMECAs, system and production availability models (RAM models), and package reliability models;
- identify actions to address any new risks to reliability, integrity, and maintainability achievement arising from the changes;
- update the RIAD;
- all reliability and integrity data generated during the field development project should be collated into the overall RIAD.

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.

- **Plan.** Schedule development and review of procedures and assessment of associated risks during detailed design as this may identify required design improvements. Relevant members of the design team (operator, supplier, sub-supplier) and the operations team should be used to inform/support the activities at each of the MATIC stages.

- **Implement.**
  - Implementation at each MATIC stage includes:
    - implementation of RIM activities (e.g. FMECA, P-FMECA) as part of development of the MATIC procedures;
    - inclusion of any identified risk management actions arising in the MATIC procedures (e.g. provision of installation team training and experience through involvement in SIT);
    - implementation of the risk management actions as part of implementing the MATIC procedures;
    - verification that the risk management actions have been carried out by regular monitoring of progress and compliance (by supplier, installer, and end user);
    - audits of vendors and suppliers to ensure proper procedures are constructed/adhered to;
    - capturing baseline data (e.g. valve P-t footprint) for comparison with data acquired during operations.
  - Both configuration and performance data should be recorded during implementation of the MATIC procedures (see B.11). A FRACAS database (or similar) for the asset should be established at this stage.
  - Auditable documentation should be created to provide assurance that risk management activities and verification processes and practices have been undertaken as planned by all parties. This should be per equipment/serial number and includes the following.

- **Manufacture and assembly—manufacturing records book.**

- **Testing—FAT, SIT, and qualification records:**
  - include all pertinent information (e.g. calibration, settings, results, etc.);
  - document that equipment has been restored to the correct (nontesting) configuration on completion of the testing.

— **Installation and commissioning**—installation and commissioning procedure records.

  — Any deviations should be included along with the disposition adopted (nonconformance report and/or MOC may be required).

— **Evaluate**.

  — Following creation/review of each MATIC procedure, revisit the procedure technical risk level and evaluate against agreed risk acceptance criteria (see B.5).

  — Following implementation of the procedure, evaluate any additional risks introduced during the procedure against risk acceptance criteria (e.g. as a result of delays). This should include a review of any associated anomaly management plans and the reliability/integrity analyses thus far.

— **Feedback**. Information generated during the MATIC stages should be collated for each package and captured in the RIAD (see B.6).

  — All relevant information generated at the supplier's site should be collated by the supplier into the package RIAD for subsequent integration into the RIAD for the subsea asset as a whole by the operator project team.

  — On delivery of equipment, the package RIAD should be included with the package documentation delivered by the supplier to the installer.

  — The subsea asset RIAD should also be updated with project-level activities (e.g. sparing/vessel updates to subsea system production availability analysis).

  — The RIAD for the asset should be updated by the installation team following completion of SIT and installation.

  — The RIAD for the asset should be updated by the commissioning team ahead of handover to operations.

  — The information presented within the RIAD should:

    — summarize the reliability and integrity risk management activities implemented together with the arising MATIC procedure improvements identified and incorporated;

    — demonstrate that the resultant procedure improvement scope of work has been carried out by the supplier/installer.

  — Feedback step should report any lessons learned that could be of benefit to future projects including lessons learned from previous operations (see B.12).

C.6.3 Additional Stage-specific Risk-based Scope of Work

C.6.3.1 Category A (Very High Risk) and B (High Risk) Procedures

In addition to the generic activities:

— the capability of potential installation contractors to effectively assess and deliver against the reliability and integrity requirements should be considered as part of the contractor selection process along with more the more standard selection criteria (see B.3);

— undertake a P-FMECA (see B.7) to identify potential failures that could occur during each step of the procedure and alter the procedure to remove each failure possibility. Whenever possible, each

procedure step should include a positive record that action was carried out correctly; for critical steps/actions this may include additional witness;

— confirm that all procedural related actions from design/earlier MATIC stage FMECAs, 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;

— assess each component and assembly qualification status against project functional integrity/integrity management and reliability requirements and incorporate all outstanding qualification activities into the relevant MATIC procedure (e.g. extended testing at SIT and as part of other system function testing);

— installation procedures should be used as much as possible during SIT to identify any problems that could occur during installation and hence any improvements needed;

— apply stress screening and highly accelerated stress screening (HASS) techniques to detect and eliminate defects introduced during manufacture of electronics and control systems;

— 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 and integrity;

— identify systems and processes for data management and storage during the MATIC stages and through operations. 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).

C.6.3.2 Category C (Medium Risk) and D (Low Risk) Procedures

In addition to the generic activities:

— 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 confirm there is no potential for any problems to occur during installation;

— review assumptions and output from previous stage FMECA and reliability/availability analysis to ensure that all decisions concerning integrity management are appropriate and acceptable to the achievement of reliability and integrity;

— confirm systems and processes are in place for data management and storage during the MATIC stages and through operations.

C.7 Operations—Normal Operations

C.7.1 General

The normal operations DPIEF loop applies to the periodic (typically annual) integrity management campaigns.

Reliability, integrity, and technical risk management is at the **procedural level** (e.g. operational procedures, etc.).

The reliability and integrity activities relating to operations start before the end of MATIC whilst detailed procedures are being written both in relation to production and integrity management to ensure that all equipment is operated correctly and within its acceptable limits.

For any new operational procedures associated with new technology, undertake a detailed P-FMECA (see Table B.3) to identify potential failures that could occur during each step of the procedure and alter the procedure to remove each failure possibility (see B.7). Whenever possible, each procedure step should include a positive record that action was carried out correctly; for critical operations, this may include additional witness.

For all equipment items and associated operations procedures, detailed risk assessments should be undertaken to support identification of the required RIM activities during operations (see B.7). Where possible, the risk assessments should be an update of design assessments undertaken earlier by the project team.

RBI methodologies may be used to determine required inspection frequencies based on the identified threats from the risk assessments (see API 580).

RCM may be used to identify appropriate maintenance and intervention strategies based on the identified failure consequences and subsequent analysis to identify the best value strategy.

At the end of each integrity management campaign, results arising from reports from the various integrity management activities (inspections, monitored data, tests, etc.) should be collated, assessed, evaluated, and summarized in the RIAD to provide feedback to management and provide and input to the next integrity management campaign.

C.7.2 Additional Stage-specific Generic Activity Guidance

— **Define System Taxonomy and Segmentation.** At completion of design the full subsea system should be defined and if required, updated during the MATIC stages (see CM in B.11).

  — System definition should be at equipment unit (assembly) level (e.g. manifold) and at subassembly/component level (e.g. valve).

  — The complete system, including pipelines and flowlines, should be subdivided into segments to support identification of specific integrity management activities for all locations, equipment, and processes. Segmentation may be based on the configuration of the system, the threats to the system, and methods of data acquisition or inspection.

  — Generally, the system architecture will not vary through life unless modifications are carried out (see C.8). This should be confirmed as part of the regular DPIEF cycle periodic review and the configuration data updated accordingly.

— **Identify Technical Risk.**

  — The TRC for each subassembly/component should have been identified as part of the project activities. The TRC provides the operations team with an indication of which equipment items are likely to require additional RIM activities above those normally implemented (e.g. more frequent inspection during early life).

  — For all equipment items and associated operations procedures, detailed risk assessments (e.g. IM-FMECA, P-FMECAs, HAZOP, etc.; see B.7) should be initially undertaken to support identification of the required RIM activities during operations. Where possible, the risk assessments should be an update of design and process assessments undertaken earlier by the project team. These risk assessment should then be periodically updated.

  — The end user (operator/operations team) of the equipment and procedures should participate in or agree the results of these assessments.

- **Goals and Requirements.** The overall goals and requirements for the asset probably remain unchanged at this stage. However, detailed operations goals and requirements should be developed to ensure that equipment operation and processes will meet reliability and integrity goals and requirements (by avoiding/controlling any actions that could cause immediate or later failure); see B.3. This should include:
  - requirements for integrity management activities (e.g. pipeline pigging frequency);
  - key performance indicators for both the equipment and the integrity management activities (e.g. compliance with the ITMM plan, number of deviations outside of operating/design intent).
- **Strategy.** The strategy at this stage should outline how the operations team deals with potential failures.
  - The integrity management and maintenance strategy should be based on a rigorous approach, such as:
    - RBI;
    - RCM.
  - Depending on failure consequences and risk, integrity management and maintenance strategy decisions may include:
    - replace when condition falls outside safe operating limits (SOLs) (condition-based maintenance);
    - replace before failure (scheduled replacement);
    - run to failure (breakdown maintenance);
    - do not replace (e.g. lock valve in open/closed position if this does not affect integrity).

      NOTE Replacement before failure (scheduled replacement) is not normal maintenance practice for equipment located on the seabed but may be appropriate for topside elements of subsea equipment. There may be opportunistic replacement before total system failure if component failure results in lost redundancy.
  - Where obsolescence has been identified as a risk, the maintenance strategy should integrate with the obsolescence strategy and the obsolescence management plan (e.g. “last time buy” of components at risk to obsolescence).
- **Scope of Work.** The IM-FMECA is the key tool used to determine the initial ITMM plan and the subsequent updating of the plan following periodic RIM campaigns.
  - Activities to be included in the ITMM plan should be identified before the start of operations and reviewed periodically following RIM campaigns (see Annex D) to provide assurance that the reliability and integrity goals and requirements for the asset are and can continue to be achieved.
  - Scope of work should include:
    - development/review of IM-FMECA to determine/confirm the ITMM plan including activity extent and frequency;
    - gap assessment of required data to available data and identification of additional integrity management activities required to address gaps;

  - equipment risk-based activities identified in C.7.3;
  - development/review of reliability analysis and implementation of procedures for required inspection, monitoring, sampling, and testing (see D.2);
  - development/review of reliability analysis and implementation of procedures for defined maintenance activity;
  - development/review of reliability analysis and implementation of procedures for data collection and management (see B.11), including use of a FRACAS database (or similar);
  - development/review/implementation of procedures for performance data analysis (see B.11 and D.4).
- Any activities in the ITMM plan that involve human intervention should be backed up by HAZID/HAZOP to ensure any risks to the safety of personnel are identified and managed appropriately.

- **Plan.**
  - Communication of the subsea asset team with other functional discipline owners, such as wells and drilling, topsides facilities and structural owners, so as to ensure all relevant parties understand the ITMM task scope, integrity limits (e.g. ensuring monitoring alarms are set to the lowest specified across the system), and objectives and that any relevant scopes can be added or interfaced.
  - Integrating planned activities, where appropriate, with maintenance work for other related systems (e.g. for topsides) to ensure that there is alignment in relation to scheduling, personnel on board, etc.
  - Defining work pack contents for each ITMM activity, including drawings and acceptance criteria.
  - Ensuring that all tasks have clearly defined QC requirements, data management requirements, reporting requirements, and anomaly limits.
  - Working with contractors where appropriate to ensure competencies are available to perform activities specified in the ITMM plan (e.g. inspection contractors, to ensure that work plans are prepared that fully address integrity, safety, and QC requirements).
  - Criteria for defined anomaly reporting limits, e.g.:
    - required assessments;
    - required time frames for completion of assessments;
    - baseline test data.
- **Implement.** Implement the integrity management activities included in the ITMM plan:
  - required inspection, monitoring, sampling, testing, and maintenance;
  - data collection, management, and storage;
  - performance data analysis.
- **Evaluate.** Evaluate the performance data against acceptance criteria (see B.5), including:
  - assessment of equipment reliability and integrity performance against goals and requirements;

- assessment of performance in terms of leading and lagging indicators against acceptance limits;
- evaluation of inspection and integrity monitoring results, to assess the effectiveness of the integrity management activities and to define trends and acceptance limits on trends;
- the assessment of any anomalies within the defined required time frame (e.g. inspection time frame). This should consider:
  - the design intent;
  - the operational environment (both external and internal);
  - processes used.

NOTE Anomalies may be picked up by routine ITMM tasks or by nonroutine operational events or in-service failures. The assessment process is to be sufficiently robust to collect these data and assess accordingly.

- Where performance data do not meet acceptance criteria, corrective action should be implemented and quality nonconformance reports should be generated as required to:
  - investigate and document the root cause requiring corrective action to enable identification of appropriate corrective action(s);
  - document and disseminate lessons learned;
  - implement the corrective action (see C.8).
- Based on the annual integrity report and other appropriate assessment completed during the execution of the procedure, the need to review the documented system, FMECA, and ITMM plan should be clear. The actions associated with this should be evaluated and completed as required.
- A thorough review of the program should be considered on a frequency not recommended to exceed 5 years.

NOTE Internal or external audits, regulatory findings, or other applicable advances in industry guidance may also act as input to the decision to revise the subsea reliability, integrity, and technical risk management program.

- **Feedback.** The RIAD for the subsea system should be updated to provide ongoing reliability and integrity assurance for the asset. The RIAD should be as concise as possible and represent “routine” data as key performance indicators rather than repeating large volumes of data reported elsewhere (see B.6).
- **Goals, Requirements, and Strategy**. Refer to the overall integrity management and maintenance strategy in relation to reliability and integrity goals and requirements.
- **Evidence**.
  - Provide evidence that the equipment is fit for service.
  - Refer to results from analysis of data obtained from inspection, monitoring, sampling, and testing.
  - Provide a summary of the management of anomalies including management effectiveness.
  - Provide a summary of nonconformance reports.
  - Provide a summary of how any procedural/human failures have been managed.

- Reliability and integrity claims—provide a statement for the asset including:
  - the known condition of the subsea asset;
  - the predicted life expectancy of the equipment;
  - the extent to which the design intent is being met;
  - the reliability performance and effectiveness of all system barriers to failure.
- Where this reliability and integrity information is not available, the reason why should be identified together with the planned corrective action.

- Feedback step should 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); see B.12.

C.7.3 Additional Stage-specific Risk-based Scope of Work

C.7.3.1 Category A (Very High Risk) and B (High Risk) Equipment

In addition to the generic activities:

- incorporate enhanced inspection and monitoring during early life to manage any uncertainty in reliability and integrity performance;
- use a final multidiscipline review by an independent entity (to the project, supplier and operator) with direct operational experience of similar systems;
- identify the operations team experience and any necessary training (e.g. consider involvement in SIT);
- identify any additional requirements for anomaly management, recognizing the novelty of the technology and/or limited operational experience (e.g. time frame for reporting);
- identify appropriate data analysis techniques and their frequencies recognizing the novelties and uncertainties associated with the equipment together with the agreed key performance indicators, for example Pareto or trending analysis;
- where possible trending of data should be used to identify the initiation of failure mechanisms ahead of the equipment exceeding operability or destruct limits;
- analysis of performance data should be used to identify opportunities for reliability growth—reliability growth analysis can be used to support this;
- where reliability and integrity performance does not meet requirements for the subsea asset, an RCA should be undertaken to identify both the root cause of the failure and appropriate corrective action—this applies to:
  - single failure or underperformance events that have a significant impact on integrity and availability;
  - frequently occurring, less significant events that have a cumulative impact on production availability.
- undertake an annual review of the integrity management program of work, to identify how effective the program is and if any changes in the integrity management are required (e.g. less or more frequent inspection).

C.7.3.2 Category C (Medium Risk) and D (Low Risk) Equipment

In addition to the generic activities:

— review the operations team experience and any necessary training (e.g. consider involvement in SIT);

— review requirements for anomaly management, to ensure continued relevance (see B.11);

— analysis of performance data should be used to identify opportunities for reliability improvement.

C.8 Operations—Corrective Action

C.8.1 General

Reliability, integrity, and technical risk management during the corrective action loop addresses:

— any required changes to the subsea equipment;

— any required changes to the operational and integrity management procedures;

— any intervention procedures used to implement the corrective action.

Any corrective action required during operations should be implemented through a corrective action DPIEF assurance cycle.

For some corrective actions, it may be more appropriate to treat the corrective action as a field upgrade. In this instance, the field upgrade should be treated as a project and follow the guidance for projects in C.2 to C.6.

C.8.2 Additional Stage-specific Generic Activity Guidance

A TRC assessment should be carried out using the appropriate table from Annex A.

The assessment of technical risk should reflect the type of corrective action to be made and the impact of this on the wider system utilizing the operator's MOC process (see B.13).

Additional stage-specific guidance for generic activities includes the following.

— **Lessons Learned.** Corrective actions should address relevant lessons learned:

  — from failure investigations (e.g. RCA) related to the corrective action;

  — from similar issues with other subsea systems and operations;

  — from similar intervention procedures.

— **Define System and Segmentation.** Update the system configuration data to reflect any changes to be made in the defined system or its segmentation for integrity management.

— **Identify Technical Risk**. Identify the technical risks associated with the corrective action. The operator of each subassembly/component should either participate in the risk assessment or verify the supplier/contractor assessment. Risk assessments may include:

  — TRC assessment for replacement equipment in conjunction with equipment suppliers (see Annex A);

  - TRL assessment for replacement equipment in conjunction with equipment suppliers (see B.10);
  - TRC assessment for any new or changed MATIC procedures (see Annex A);
  - IM-FMECA, P-FMECAs, and HAZOP for changed or new operations procedures (see B.7).

- **Goals and Requirements**. Goals and requirements should be defined for the corrective action procedure. The overall goals and requirements and wider strategy for RIM of the subsea asset should be reviewed in light of the required corrective action. Goals and requirements may include:
  - reliability and integrity goals and requirements for changed-out equipment;
  - reliability and integrity goals and requirements for new/changed procedures;
  - reliability and integrity goals and requirements for any associated MATIC activities;
  - requirements for regulatory approval of planned intervention actions.

- **Strategy.** The strategy should consider how the corrective action will be managed as part of the wider operation of the subsea asset, e.g.
  - immediate implementation of corrective action required;
  - intervention as part of existing planned intervention activities;
  - continue to operate but plan for corrective action in the event of escalating risk.

- **Define Scope of Work.** The scope of work should identify the required RIM activities associated with the corrective action. These may include the following.
  - Equipment and procedure risk-based activities as defined in C.8.3.
  - Design activities (see also C.5) including:
    - preparing equipment specifications, if not available from design, which state clearly functional and operating environment goals and requirements.
  - MATIC activities for replacement/changed/new equipment (see also C.6) including:
    - reviewing the preservation of spare parts;
    - reviewing any pre-installation tests completed to ensure that the spares and any tooling functions as required and do not have hidden-failure potential;
    - technical risk assessments (e.g. FMECA/P-FMECA/HAZOP) for the repair/installation procedure, as part of development of the procedure, to ensure that the repair/installation does not impact on the reliability and integrity of interfacing equipment and that the repair is both safe and efficient with minimum impact on production availability.
  - Operations activities for replacement/changed/new equipment:
    - developing/reviewing the ITMM plan (see Annex D) for integrity management of replaced/changed/new of equipment, and document the corrective work and manage in accordance with the knowledge management system procedure requirements;
    - reviewing the preservation of spare parts.

- **Plan**. Develop a plan in accordance with MOC procedures for implementing the reliability and integrity activities associated with the corrective action (see B.4), including:
  - liaising with OEMs, where long-term support agreements are in place:
    - OEM parts should be used for replacement where possible;
    - the impact of non-OEM parts should be considered as part of MOC where applicable;
  - reviewing QC plans (e.g. scheduling of required MATIC activities prior to offshore transport).
- **Implement.** Implement the reliability and integrity activities included in the corrective action plan including:
  - implementation of RIM activities (e.g. FMECA, HAZOP) as part of design modifications and/or development of the corrective action procedures (e.g. installation/repair procedures);
  - inclusion of arising identified risk management actions in the design or corrective action procedures;
  - implementation of the risk management actions as part of implementing the corrective action procedures;
  - verification that the risk management actions have been carried out by regular monitoring of progress and compliance (by supplier, installer, and end user);
  - an RCA procedure to investigate the root cause of the failure.
- **Evaluate.** Following development of procedures for the corrective action, revisit the procedure technical risk level and evaluate against agreed risk acceptance criteria (see B.5). Following implementation of the corrective action procedure:
  - ascertain whether the corrective actions conflict with risk acceptance criteria and update corrective actions or acceptance criteria accordingly;
  - update the original risk assessment initiating the need for corrective action to reflect the corrective action implemented and re-evaluate against the risk acceptance criteria;
  - evaluate any additional risks introduced during the corrective action procedure against risk acceptance criteria (e.g. as a result of delays). This should include a review of any associated anomaly management plans.
- **Feedback.** The RIAD for the subsea system (see B.6) should be updated to reflect the corrective action implemented including:
  - any updated goals, requirements and strategy for the asset including any new integrity management requirements;
  - any new/updated reliability and integrity assessments for the asset.

  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); see B.6.

C.8.3 Additional Stage-specific Risk-based Scope of Work

C.8.3.1 General

A specific scope of work should be developed for management of reliability and integrity in the corrective action loop from the generic activities defined for each equipment technical risk category as outlined below.

C.8.3.2 Category A (Very High Risk) and B (High Risk) Replacement Equipment

In addition to the generic activities:

— implement the organization's MOC procedure for the introduction of new equipment;

— as part of any design changes, identify and understand the original design intent and operational environment and reflect this in the corrective action plan and specifications;

— identify any changes to interfaces with the existing system that may impact the reliability and integrity performance of either the replacement equipment or the wider system (e.g. interface FMECA) to identify any potential failure modes and associated risk management actions;

— where spare parts are to be used, review their condition and implement any pre-installation tests or inspections necessary to ensure the spare will still function as required;

— update the configuration data for the asset to reflect the equipment changes;

— identify a suitable ITMM plan (see Annex D), including activity extent and frequency, linked to the earlier FMECAs and other risk assessment outcomes to ensure all residual risks are controlled for the life of the equipment and asset;

— for assets where similar subassemblies/components are already installed that could also require the same corrective action, identify a strategy for implementing the same corrective action for these items ahead of their potential failure.

C.8.3.3 Category C (Medium Risk) and D (Low Risk) Replacement Equipment

In addition to the generic activities:

— implement the organization's MOC procedure for the introduction of new equipment;

— as part of any design changes, identify and understand the original design intent and operational environment and reflect this in the corrective action plan and specifications;

— confirm there are no changes to interfaces with the existing system that may impact the reliability and integrity performance of either the replacement equipment or the wider system (e.g. through a review of existing interface FMECA);

— where spare parts are to be used, review their condition and implement any pre-installation tests necessary to ensure the spare will still function as required;

— update the configuration data for the asset to reflect the equipment changes;

— review the ITMM plan, including activity extent and frequency, to confirm that it is still appropriate and sufficient;

— for assets where similar subassemblies/components are already installed that could also require the same corrective action, identify a strategy for implementing the same corrective action for these items ahead of their potential failure.

C.8.3.4 Category A (Very High Risk), B (High Risk), and C (Medium Risk) Replacement Integrity Management/Operations Procedure

In addition to the generic activities:

— identify any risks of continuing to operate with previous integrity management or operations procedure to define how long production can continue for;

— implement the organization's MOC procedure for the introduction of new/changed procedures;

— implement relevant risk assessment activities implemented at the start of the normal operations cycle (e.g. P-FMECA, HAZOP);

— define a strategy for incorporating new procedures into operations. This may include the impact on the rest of the system or identification of training;

— identify the effects of the novel or modified procedure on both integrity and production availability to ensure the operation is still in line with the system goals and requirements.

C.8.3.5 Category A (Very High Risk) and B (High Risk) Corrective Action Intervention Procedures

In addition to the generic activities:

— undertake a risk assessment associated with the cause of the corrective action to identify the risks of continuing to operate until the corrective action is implemented and a time frame for implementing the corrective action;

— implement relevant activities recommended for Category A and B installation and commissioning procedures (e.g. application of P-FMECA);

— identify any vessel, tooling, and resource requirements and any potential impact of their availability on the time frame for implementing the corrective action and hence any potential impact on meeting production availability requirements;

— identify any necessary operation team training (e.g. consider involvement of third parties with relevant experience);

— update the configuration data for the asset to reflect the corrective action.

C.8.3.6 Category C (Medium Risk) and D (Low Risk) Corrective Action Intervention Procedures

In addition to the generic activities:

— undertake a risk assessment associated with the cause of the corrective action to identify the risks of continuing to operate until the corrective action is implemented and a time frame for implementing the corrective action;

— implement relevant activities recommended for Category C and D installation and commissioning procedures (e.g. review of procedure);

— confirm required vessel and resource availability to identify any potential impact on the time frame for implementing the corrective action and hence any potential impact on meeting production availability requirements;

— review operation team experience and any necessary training;

— update the configuration data for the asset to reflect the corrective action.

Annex D
(informative)

Integrity Management Data Collection

D.1 Considerations at the Design Stage

From the point of view of the operators, there are three broad methods for acquiring data. These are:

— monitoring;

— sampling;

— testing.

Each of these is expanded in the sections below. Project teams should consider the likely requirements for such data, for the purpose of managing reliability and integrity during operations, and should, by design, make suitable provision for acquisition.

D.2 Methods of Data Acquisition

D.2.1 Monitoring

— Monitoring refers to any continuous (or quasi-continuous) data stream obtained from any part of the system via the electro-hydraulic control system. (Note that modern systems incorporate fiber optics to provide high band width paths for data transmission.) These data are collected by the distributed control system data logger, primarily for production control, and should include the following.

— Temperatures:

  — well—downhole and at surface (tree);

  — well bay or header;

  — flowline inlet;

  — top of riser;

  — test or first stage separator.

— Pressures:

  — well—downhole and at surface (tree);

  — wellbay or header;

  — flowline inlet;

  — top of riser;

  — test or first stage separator;

  — high-pressure/low-pressure (HP/LP) fluid delivery (topsides);

  — HP/LP fluid receipt (at manifold);

  — HP/LP fluid receipt (at well).

— Flow rates:

  — individual tree throughput (ideally a MPFM will be fitted for each well);

  — manifold export (ideally a MPFM will be fitted for each flowline);

  — test or first stage separator;

  — fiscal metering;

  — HP fluid usage;

  — LP fluid usage;

  — injection of chemicals.

Other monitored parameters may include:

— CO_2 level;

— H_2S level;

— dewpoint (gas);

— water cut;

— density of product;

— viscosity of product;

— online erosion/corrosion monitoring (e.g. probes—sand production, corrosion, etc.; and corrosion monitoring spools);

— insulation resistance in umbilical signal and power lines.

These data provide the control room operators (CROs) with a real-time picture of the system performance, but the data are also beneficial for RIM. For instance, an increasing pressure differential between the flowline inlet and the top of the riser could indicate wax buildup, severe wall roughening (internal corrosion), or a partial blockage (possibly a hydrate). Increasing gas production in a multiphase system could indicate encroaching slugging conditions. Fluctuating pressures could indicate slugging or might indicate sand production in bursts. It is not possible to list every possible problem, but the CROs should be instructed to challenge all results from the point of view of threats to system availability or integrity.

NOTE “Quasi-continuous" refers to data that are logged locally and must then be downloaded in batches. This might apply to sand or corrosion probes.

In addition, there will be a continuous feedback from the subsea production control system itself, including self-diagnosis checks. These data are not generally provided to the CROs, but subsea engineers should have the data reviewed frequently by a controls engineer to identify any incipient faults that could lead to downtime. It should be possible to access these data from an office onshore.

D.2.2 Sampling

Sampling refers to obtaining samples of product, lift gas, injection water, hydraulic control fluid, injection chemical, and carrying out tests to obtain data. Examples are given below.

— product—water cut, bulk solids, chlorides, iron and manganese counts, wax, asphaltene, acid gases, organic acids, residual chlorine;

— lift gas—H_2S level, dewpoint;

— injection water—O_2 levels, residual O_2 scavenger (e.g. bisulfite), sulfate reducing bacteria counts;

— hydraulic control fluid—cleanliness (in both the supply containers and the HPU reservoir);

— injection chemical—cleanliness, concentration;

— separator residues—after cleaning—corrosive species, sand, wax, asphaltene;

— pig debris (“pig trash”)—corrosive species, sand, wax, asphaltene, hydrates;

Sampling is generally carried out by the production technicians on the platform, to a defined schedule, as with sampling of on-platform production. The frequency of sampling will depend upon:

— the criticality of the parameter (from the FMECA);

— the historical rate or frequency of variation of the value;

— the proximity to the SOL or alarm set point;

— the repeatability of the readings (the greater the variability, the more data points required);

— company operating requirements.

Some, such as separator or pigging residues, can only be sampled as opportunity arises. Most would be sampled at intervals no longer than weekly. Analysis of samples is frequently carried out by a production chemist.

D.2.3 Testing

Testing refers to activating a process for the sole purpose of confirming that initiation and function match the performance standard. Tests are prescribed to be conducted at specified intervals, and are typically included in the topsides testing schedule (since the tests are initiated from the control room, or locally, topsides). Examples of equipment that may require testing include:

— emergency shutdown valve (ESDV);

— subsea isolation valve (SSIV);

— underwater safety valve (USV);

— instrumented pressure protection system valves.

These tests confirm that:

— initiating a demand leads to a signal being sent to the actuator;

— the actuator moves the gate or ball (partial closure test);

— the gate or ball closes to the stop (full closure test);

A full closure test also permits a leak-off test to be carried out.

It is also possible to obtain a valve “footprint”—the hydraulic profile of the closure (or opening)—and to measure the usage of hydraulic fluid, provided positive displacement flow meters are provided (which is strongly recommended). The footprint and usage can be trended from test to test. Ideally, a baseline test will have been carried out at commissioning so that “in-service” footprints, etc., can be compared to the “as installed” footprint.

Testing does not have to be limited to the ESDV, SSIV, etc. For example, while it is not normal practice to close in the system to test an isolation valve in a manifold, if the valve has to be stroked for operational reasons, the footprint and hydraulic usage should be recorded and reviewed. Pigging valves will be opened prior to a pig run; again, the footprint can be recorded. Calibration of choke valves can also be seen as a form of testing.

Testing is not limited to valves. Many components of the subsea production control system can be tested as part of ongoing reliability confirmation. Chemical injection metering and rate control components can be tested.

During the design phase, the operations subsea engineer, controls engineer, and reliability and integrity engineer should be involved and should define what testing they believe will be required so that the provision is made during fabrication and installation.

D.3 Considerations During Operations

Monitoring, sampling, and testing should be carried out during steady-state operations, as noted above, and used for building up a model of the subsea system, its characteristics, and condition. (Note that this does not necessarily refer to a comprehensive numerical model, but a consistent understanding of the way the system behaves.) The requirements, in terms of activities, frequencies, responsibilities, outcomes, and key performance indicators, together with maintenance requirements—i.e. those activities required in light of findings from those activities, to maintain reliability or integrity—should be combined into the ITMM plan. Some operators retain this as a rolling (typically 5-year) plan. Inspection is addressed in D.5 below.

D.4 Data Acquisition During Specific Activities

The guidance on monitoring, sampling, and testing above refers predominantly to steady-state production operations. There are certain activities that occur on occasion, which require much closer monitoring of certain data and, possibly, testing. Such activities include:

— field start-up;

— field shut-in;

— blowdown and depressurization;

— pigging (operational or intelligent);

— bull-heading;

— simultaneous production and drilling;

— intervention and maintenance.

During field start-up, when valves are cracked open, fluid temperatures fall very low due to Joule-Thomson cooling. Low temperatures can cause embrittlement of steel, and a minimum design temperature will have been defined (and Charpy tests carried out on this basis). This will be defined as an SOL, and the CRO should monitor temperatures continually to ensure that this SOL is not exceeded. Low temperatures can also lead to hydrate blockages, and it is usual to inject critical points in the system with methanol or glycol to prevent this. The CRO should check that the methanol has been distributed correctly and should monitor

pressures continually to identify any early indications of possible blockage. Various well parameters will also be monitored frequently to ensure that the start-up is stable.

Field shut-in is less critical and, in many cases, is automated. The CROs should monitor the distribution of methanol (or glycol) and monitor temperatures and pressures during cooldown. In many deep water facilities, it is not possible to manage the shut-in outside the hydrate region because hydrostatic pressure is too high. In this case, great care must be taken to avoid hydrate blockage, although this may not become apparent until start-up.

The issues surrounding blowdown are similar to shut-in, except that gas may have to be flared in order to depressurize quickly enough. In this case, flow rates become important.

During pigging operations, pigs can become stuck, the evidence being similar to any other blockage. Pig speed is controlled by flow rate and so this becomes an important parameter. Valve status is also important; a pig attempting to transit a valve that is not fully open can do considerable damage. Pig signalers may be used to flag up when a pig passes a particular point in the line.

Bull-heading requires that reservoir pressure is overcome. (If the subsea system has not been designed for this, it may be that the design pressure is too low, so that the bull-heading must not be carried out.) Valve status (ensuring the correct routing of the fluids) is important, and it is important to monitor the temperatures and pressures as the activity progresses. Note that bull-heading tends to rapidly cool a flowline while it remains at high pressure, and this can generate abnormal stresses that could cause failure of latent manufacturing defects; therefore, the CROs should always bear in mind the possibility of a leak to the environment.

Simultaneous production and drilling is a relatively unusual activity. The requirements will be specific to the particular arrangement, and the critical parameters should be defined in the operating procedure.

During intervention and maintenance, the CROs should have a copy of the task procedure. They may be required, for example, to take a variety of readings, to depressurize or pressurize parts of the system, to inject chemicals at a particular location, or to operate a particular valve. In every case, they should monitor all relevant parameters. If the intervention is on a tree, they may be required to hand over control of the well to the intervention team. In such cases, the procedure covering well handover from operations to the intervention team should be followed, to include signing off the Well Handover Certificate, and likewise on return to operations control.

As a general rule, during these activities as with normal production, the CROs should be continually vigilant for any parameter that appears to be trending away from the norm.

D.5 Inspection

D.5.1 General

Some of the components within a subsea development will be subject to ongoing condition monitoring. However, many of the components within the system will not lend themselves to condition monitoring and therefore these items will need to be subject to a routine internal or external inspection regime. The inspection regime will look for evidence of the following conditions:

— corrosion;

— erosion;

— leaks;

— damage;

— coating degradation;

— cathodic protection (CP) system degradation;

— marine growth buildup;

— seabed movement;

— displacement or movement of subsea infrastructure;

— debris or dropped objects.

D.5.2 Methods For Determining Inspection Frequency

D.5.2.1 General

Several methods are available and can be used when setting an inspection strategy. Inspection frequencies may be set based on one or more of the following methods.

D.5.2.2 Time-based

Inspection intervals may be set based on elapsed time in service. This method of setting inspection frequencies may be recommended by manufacturers for specific items of equipment or may be required by specific legislation. Otherwise, it is likely to be set according to available operating statistics (e.g. MTTF).

D.5.2.3 Condition-based

Condition monitoring of parameters can indicate when a change has occurred in a system. This indication of change can be used to initiate an inspection. Alternatively, the observed condition of an item of equipment seen during an inspection can be used to modify an existing inspection plan (i.e. intervals can be made more or less frequent, depending on the findings of an inspection).

D.5.2.4 Risk-based

This form of inspection strategy setting follows on from a risk assessment, which will consider both the probability of a failure mode occurring and the consequences that would follow that event (financial, environmental, societal). The strategy is then set so that the highest risk components are inspected most frequently.

D.5.3 Inspection Techniques

D.5.3.1 Internal Inspection

Internal inspection is aimed primarily at identifying, and mapping, internal corrosion or erosion. ILI using intelligent pigs provides the most comprehensive data, end-to-end within the piggable flow path. Various techniques are available for general wall thickness measurement [e.g. magnetic flux leakage (MFL), ultrasonic (UT) measurement, and various eddy current (EC) methods], and tools can be configured for crack detection also (success somewhat dependent on the nature and orientation of the potential cracking).

Limited internal inspection may be achieved with tethered crawler pigs. These can be equipped with similar tools and run a distance of, typically, 500 m to 2000 m from the insertion point, depending upon the drag on the tether caused by the configuration. For example, a tethered pig might be used to inspect the girth welds in a steel catenary riser. Tethered pigs can also be fitted with video cameras, for example to inspect the carcass of a flexible riser, but an oil line will require flushing with water first.

While ILI is aimed primarily at internal degradation, it can also identify external features—e.g. external corrosion or damage—provided the wall thickness is not too great (the limit being a function of each specific technique). Some “smart pigs” can identify spanning or wax buildup, or measure out-of-straightness. Caliper pigs can provide data on restrictions or ovalization.

D.5.3.2 External Inspection

D.5.3.2.1 General

External inspection falls into two broad approaches:

— sonar mapping;

— visual inspection.

D.5.3.2.2 Sonar Mapping

Side-scan sonar (SSS) or downward-looking multibeam sonar (MBS) use multiple acoustic transmissions to create a map of the terrain and the infrastructure upon it. The data require extensive software processing to create the maps, but the output can look like a visual map. It is important that users understand that the topography is created by the quality of reflection provided by the seabed and the objects upon it, and is not a direct visual map. Accurate interpretation may require experience.

SSS or MBS will typically be deployed in either a remotely operated towed vehicle (ROTV) or an autonomous underwater vehicle (AUV). In either case, the typical transit speed enables a relatively rapid coverage. The altitude is such that sonar mapping is good for locating displacement of flowlines, burial and exposure, anchor or trawl scars, spanning, buckling, larger debris, etc., but it is generally unable to discern details such as local damage.

Sonar mapping is not applicable to the inspection of subsea infrastructure—trees, manifolds, tie-in spools, etc.—other than general mapping created by overflying a field.

D.5.3.2.3 Visual Inspection

Visual inspection is carried out almost exclusively by ROVs equipped with closed circuit video cameras. (Historically also by manned submersibles and divers; these days, divers might be used in shallow depths as an extension of intervention work, but seldom otherwise.) Increasingly, agile AUVs are being developed that can carry out both light intervention and inspection work. (AUVs may be designed to recharge their batteries from a charge point built into the subsea infrastructure.) Inspection ROVs (and AUVs) are frequently equipped with twin half-cell stabs to measure the potentials at sacrificial anodes or points of damage, as well as field strength where stabs are not possible. They can also carry specialized tooling and can combine inspection with intervention—e.g. valve actuation.

The inspection of subsea infrastructure is usually carried out visually, looking for any anomalistic condition. In addition, ROVs (and AUVs) can acquire downloads of data from remote data loggers or samples from dedicated sampling stab points.

For pipeline inspections, ROVs transit relatively slowly so that inspection is time-consuming, but ROVs work at a proximity that is suitable for investigating detail—e.g. localized external corrosion, damage, debris, etc., and the condition and degree of depletion of sacrificial anodes. Their maneuverability enables them to stop and backtrack, so that they can look at features from different angles and with different light levels. They can also take measurements (e.g. of long spans). ROVs can be equipped with pipe trackers to locate and follow buried pipelines.

Annex E
(informative)

New Technology Qualification

NOTE This annex is included to provide interim guidance until the next edition of API 17Q is published and may be removed at that time. The next edition of API 17Q is completely rewritten from the First Edition, providing more detailed guidance for the industry on new technology qualification including qualification of modified/extended technology.

E.1 Introduction

This annex provides additional guidance on the qualification of new technology. Section E.2 describes the recommended new technology qualification process. Section **Error! Reference source not found.** provides a detailed description of the expectations at each level on the TRL ladder. Section E.4 provides a brief description and comment on the degree of alignment of the API TRL 0 to 7 ladder and the alternative TRL 1 to 9 ladders used by some companies.

E.2 Technology Development Projects in Field Projects

Both initial and required TRLs should be determined for a given item of equipment early in a TQP, the aim being to raise the TRL from its initial value to the required TRL.

New technology qualification may be required at any stage of the life cycle of an asset from early design and development through to operations.

The extent to which an item of equipment is qualified for a particular application should be formally assessed to define its readiness for field operation through its TRC (see A.1) and TRL ratings (see E.4).

E.3 TQP Activities

E.3.1 General

Figure E.1 shows the main steps to be undertaken in a TQP.

E.3.2 Step 1: Requirements Planning

E.3.2.1 General

In this step of the TQP, the goals and requirements for the technology and its application together with an initial plan and qualification requirements are defined:

— develop a plan for identifying goals and requirements from stakeholders,

— elicit and validate goals and requirements,

— prepare a draft application specification document for the technology and issue to stakeholders for comment and approval,

— issue final draft of the application specification with approved goals and requirements,

— create a draft plan to initiate the TQP.

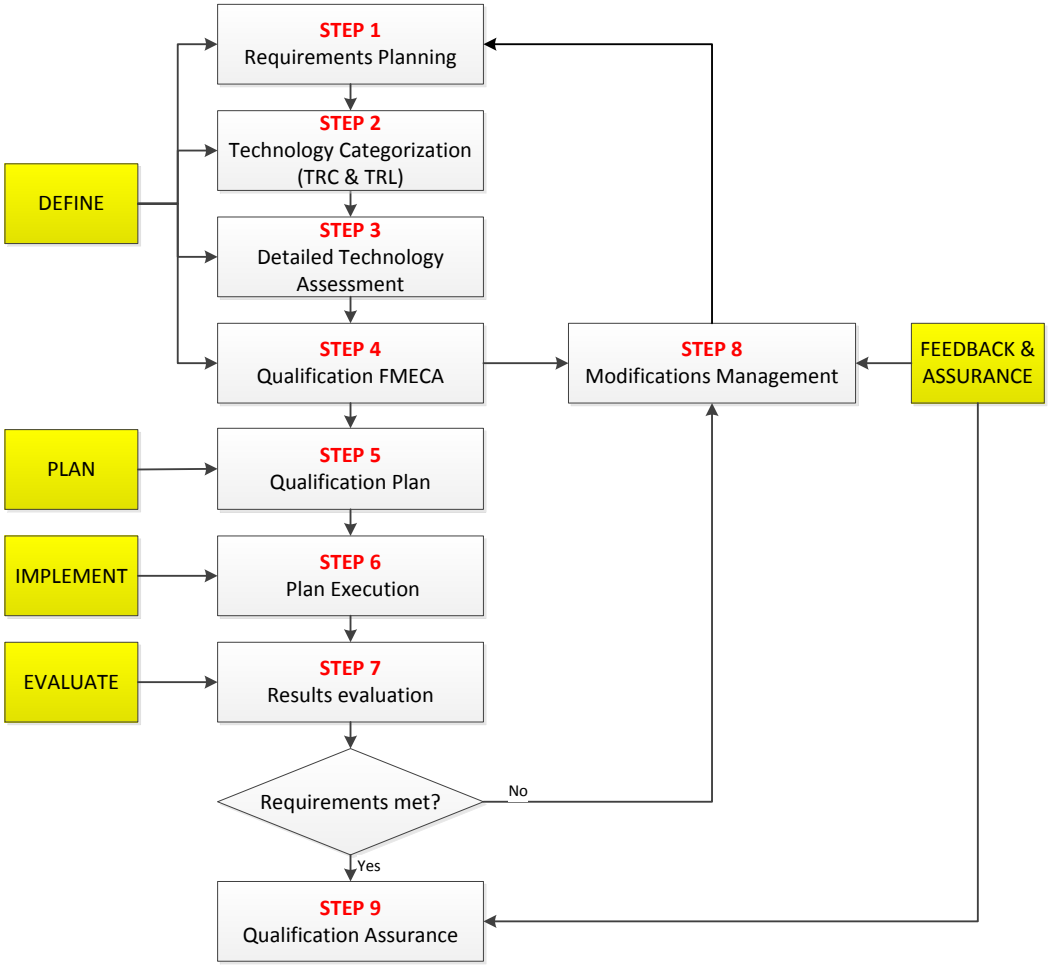


Figure E.1—Outline TQP

E.3.2.2 Technology Application Specification

The output of the requirements planning activity is the technology application specification that contains the goals, requirements, and technical risk acceptance criteria. The purpose of the specification is to provide a common set of criteria against which all qualification activities will be assessed. The specification should aim to be unambiguously and completely described through text, calculation data, drawings, and other documents. It is important that the functional and performance requirements and limitations of the technology are stated and that all relevant interfaces are clearly defined.

The technology performance goals and requirements should address, but not be limited to, the following areas:

— function and performance;

— life cycle stages to be addressed;

— design standards to be used;

— operational and process conditions;

— internal and external environmental conditions;

— equipment life;

— reliability and integrity performance;

— limit states (critical parameter list);

— qualification and technology readiness.

NOTE New technology may not be covered by established codes and procedures, and it may not therefore be clear how to qualify against existing standards or requirements.

E.3.2.3 Initial Plan

As part of the requirements planning process a high-level initial qualification plan should be created.

— Identify the qualification team and define their roles and responsibilities.

— Develop a schedule for:

  — technology categorization (Step 2);

  — technology assessments (Step 3);

  — Q-FMECA (Step 4).

The initial plan should be updated during subsequent stages of the qualification program as qualification requirements are clarified. The plan should aim to provide an indication of the level of effort and resources needed to progress the technology from initial to required TRL.

The initial plan should typically refer to:

— any specialist testing or R&D facilities that may be required during the later stages of qualification;

— any specialist skills, expertise, or training required;

— timescales for key activities and milestones within the qualification process;

— order of magnitude costs.

A TQP has the characteristics of a project. The technology qualification plan should refer to, and integrate with, the life cycle stages of the developer's technology development project.

Where the technology is to be deployed as part of a field development, TQP plans should also be integrated with the Operator's field development plans.

E.3.3 Step 2: Technology Categorization

Technology categorization is a high-level activity performed before the initiation of a qualification program to determine whether the technology will require a new TQP to be defined or whether an existing SQP can be used to qualify equipment ready for application within an operator's field development project.

The decision logic in Figure E.2 may be used to support this activity.

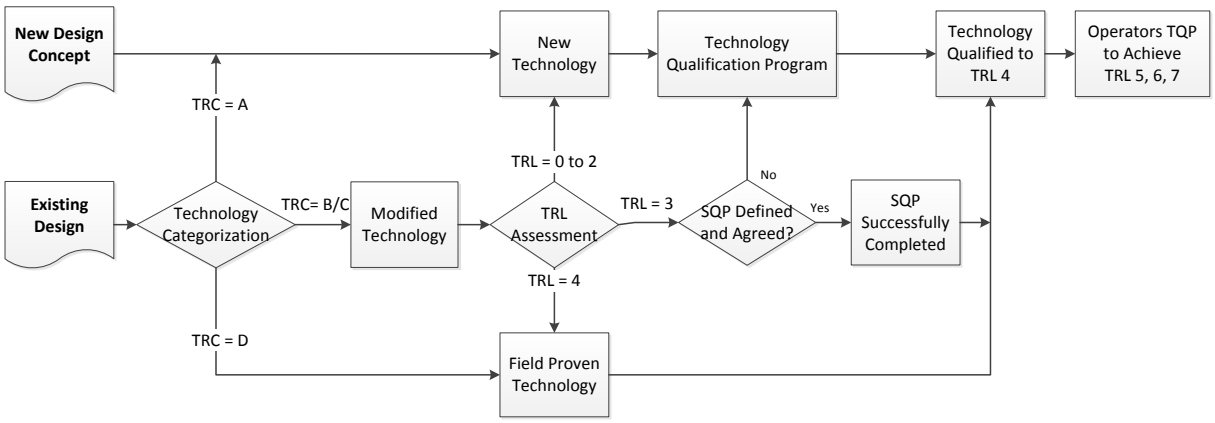


Figure E.2—Decision Logic for Selection of Qualification Process

If the technology is a new design concept, it is classed as new technology and a formal TQP should be followed.

Where the technology is based on an existing design, then an initial screening using TRC (see Annex A) should be performed:

— TRC = A: New technology;

— TRC = B or C: Modified technology;

— TRC = D: Field proven technology.

A novelty assessment screening tool such as that described in DNV-RP-A203 may be used as an alternative to TRC.

For equipment classified as modified technology, an initial high-level TRL assessment should be performed with possible qualification path decisions defined in Table E.1.

Table E.1—Dependence of Qualification Path on TRL

Readiness Level	Qualification Path
TRL = 0–2	For equipment that has not achieved TRL 3, a formal TQP should be defined.
TRL = 3	For equipment that has achieved TRL 3 but not TRL4: 1. an SQP may be applied provided that an SQP has been defined and agreed between the developer and end customer; 2. a formal TQP should be defined if an acceptable SQP has not already been defined or has not been agreed between the developer and end customer.
TRL = 4	For equipment items that have achieved TRL 4, an appropriate SQP may be used.
TRL > 4	For equipment that have achieved TRL 4, it is expected that further qualification, to achieve TRL 5 and higher, will be through the operator's TQP.
NOTE For equipment categorized as TRC = D it should be verified that there have been no incremental design or manufacturing changes that could reduce the TRL of components to levels below TRL 4.	

On completion of Step 2, the initial qualification plan created during Step 1 should be updated to reflect any changes in qualification requirements or technology requirements arising from the technology categorization activity.

NOTE SQPs are equipment specific and are not addressed in this RP. Refer to relevant API or ISO standards for guidance and details related to SQPs.

The following steps are relevant only to items following a TQP.

E.3.4 Step 3: Technology Assessment

For a technology that, following the high-level assessment in Step 2, is found to have a TRL < 4, a technology assessment should be performed to:

— fully understand the performance requirements of the technology and its components;

— identify which components of the technology are novel and which are field proven.

The technology assessment should include:

— hierarchical breakdown of the technology;

— functional analysis to identify all functions including, primary, secondary, and lower order functions together with associated required components;

— identification of performance requirements at component level, including associated reliability requirements;

— assessment of TRL for each component of the technology in the context of the functional performance requirements.

The system breakdown and subsequent assessment should be to a level of granularity appropriate to the design status, current TRL and anticipated qualification activities.

The breakdown should be at the same level of system indenture as that to be used for the Q-FMECA in Step 4.

All system boundaries should be clearly defined.

E.3.5 Step 4: Qualification FMECA

The key tool used to identify technology qualification activities is the Q-FMECA.

The purpose of the Q-FMECA is to identify or define testing or analysis activities that may be used to demonstrate the ability of the technology to meet specified functional performance requirements.

The Q-FMECA should be performed at a function level and include the following.

— system breakdown (from Step 3);

— identification of functions and performance requirements for each component (from Step 3);

— initial TRL of components (from Step 3);

— identification of all potential failure modes, mechanisms, and root causes for each functional entity examined, addressing potential deviations from performance expectations;

— identification of failure consequences;

— means of failure detection;

— identification of qualification activities needed to achieve the required TRL;

— criticality assessment of each potential failure mode.

For modifications to existing technology:

— the system breakdown should identify all elements of the technology and be of sufficient granularity to identify which items are affected by the design or application changes;

— for items affected by changes to the design or application environment, additional granularity may be required. The level of granularity should be appropriate for the anticipated qualification activities;

— the system breakdown may be used to identify combinations of items required for qualification testing as an assembly. This is useful where a specific failure mode only applies to an assembled unit or if it is not feasible to test items separately.

Q-FMECA may need to address relevant transit, storage, installation, intervention, and testing stages in addition to the operational stage of the technology.

Where underlying failure mechanisms and causes are not fully understood, Q-FMECA actions should include investigations, including those involving testing and research, to improve knowledge and understanding of failure.

Q-FMECA studies are impracticable for technology at TRL 0 or TRL 1 stage of development. Q-FMECA assessment should be deferred until TRL 2 activities or until sufficient design detail is available to support analysis.

Previous and current qualification evidence in relation to each failure mode/mechanism/cause should be identified and recorded in the Q-FMECA.

Relevant codes and testing standards may be used to support qualification testing activities where these are available and relevant. However, for some technologies, where current codes and standards are not readily available or are inapplicable, bespoke tests should be specified or developed for the purpose of qualification.

The consequence of each failure mode should be identified for the item/technology and, where known, the wider system in which it is to be deployed.

The company or operator risk matrix may be used to assign a severity level to the identified consequences.

The residual technical risks and uncertainties associated with each failure mode should be identified noting that:

— for failure modes classified as high risk, additional qualification activities should be undertaken to reduce the level of technical uncertainty and to identify design and development actions to reduce the likelihood of the failure mode occurring;

— for failure modes classified as medium or low risk, additional qualification activities may be undertaken if there is a high degree of technical uncertainty or there is value in investing in improved reliability and integrity performance.

Following implementation of identified qualification activities and follow-up actions, the technology assessment and FMECA should be updated including an update of the residual technical risk associated with each failure mode.

E.3.6 Step 5: Qualification Plan

The technology assessment (Step 3) and Q-FMECA activity (Step 4) should be used to prepare a detailed qualification plan for the technology.

All qualification actions identified in the FMECA should be converted into specific measurable and actionable activities. These may include:

— design improvements;

— analyses, modeling, or simulations;

— testing (physical);

— QA/QC requirements;

— requirements for storage, installation, intervention, maintenance, etc.;

— sparing requirements;

— operating procedure requirements.

For all activities, the detailed plan should specify:

— roles and responsibilities;

— methodology to be used for testing, simulation, or analysis;

— detailed procedures for implementing the qualification activity;

— test pass/fail criteria;

— resources required for:

  — testing and analysis activities including specialist facilities and expertise;

  — qualification assurance documentation;

  — model and data validation activities;

  — residual risk assessment;

— schedule for completion.

E.3.7 Step 6: Execution of Qualification Plan

E.3.7.1 General

The execution plan should aim to provide tangible evidence that the technology can meet specified function, performance, and reliability expectations or demonstrate the extent to which the technology meets the specified function and performance requirements.

E.3.7.2 Modeling and Assessment Methods

Where there are numerical reliability requirements, quantitative reliability assessment activities should be performed to demonstrate compliance. Examples of methods that may be considered for modeling and analysis include the following.

- Standard system reliability analysis tools including:
  - RBD analysis;
  - ETA;
  - FTA.
- Advanced engineering analysis methods including:
  - finite element analysis (FEA);
  - computational fluid dynamics (CFD);
  - multi-physics analysis.
- Advanced predictive reliability analysis methods including:
  - probabilistic FEA;
  - stress-strength interference modeling;
  - probabilistic fatigue analysis;
  - probabilistic corrosion analysis.

E.3.7.3 Testing

Qualification testing may include cycle-based testing for equipment operating intermittently or standby equipment (e.g. valves) or time-based testing for continuously operating equipment.

Reliability testing methods may include:

- reliability demonstration testing (RDT):
  - testing for a specified time or number of cycles;
  - testing to failure;
- accelerated life testing (ALT);
- HALT.

E.3.7.4 Reliability Analysis of Test Data

In order to assess reliability performance, tests should provide a record of the times or number of cycles at which failures occur, or the number of failures experienced over a specified test time interval.

Statistical analysis of cycle test data may be performed in accordance with Annex F to determine equipment failure rate.

Where tests are performed with no observed failures, standard chi-square analysis methods may be used to assess failure rate to a specified level of confidence.

Where test results include time of failure for a number of replicate tests, Weibull analysis may be used to estimate life and indicate whether the failure rate is constant or increasing with time.

E.3.7.5 Verification and Documentation of Qualification Activities

Effective assurance processes should be in place to ensure all physical tests and qualification testing procedures have been followed.

The results of all qualification activities should be documented, including all assumptions and limitations qualification assurance evidence.

The FMECA should be updated following completion of the identified qualification activities.

E.3.8 Step 7: Evaluation of Qualification Results

The results of the qualification activities should be evaluated against predefined pass/fail or risk acceptance criteria.

Root cause failure analysis (RCFA) should be performed for key component failures occurring on test to support identification of technology improvement actions.

Test data may be analyzed statistically to determine required reliability metrics such as probability of failure, failure rate, or availability. Annex F provides guidance and a description of statistical methodology for assessment of failure rate of valves to a required level of confidence. The method is extendable to many other cycle- or time-based tests.

The results of qualification activities may raise important additional information, including performance anomalies and new or unexpected failure mechanisms and causes requiring further testing.

E.3.9 Step 8: Modifications Management

Following evaluation of the qualification corrective actions should be implemented to bring about design, deployment, or operational improvements.

Any changes should be managed in accordance with the agreed MOC process and the qualification basis document updated accordingly.

Any significant design modifications will generally require further qualification work.

E.3.10 Step 9: Qualification Assurance

A qualification assurance document should be provided for new or modified technology assessed using a TQP. An example content list is shown in Table E.2.

The qualification assurance document should include written evidence of the extent to which the technology meets the requirements for its intended application with traceability to:

— requirements in the technology specification document;

— failure modes and associated mechanisms and causes relating to each requirement;

— qualification activities implemented to address each failure mode, mechanism, and cause;

— qualification evidence produced from each activity.

Table E.2—Example Contents of Technology Qualification Assurance Document

Section	Title
1	Qualification basis
2	Technology acceptance criteria
3	Technology assessment and FMECA
4	Current and required TRL
5	Qualification plan
6	Testing requirements and test pass/fail criteria
7	Test results, fault corrections, and reliability improvements including claims related to the achievement of goals and requirements
8	Residual technical risk and uncertainty
9	Conclusions and recommendations

The qualification assurance process should include an assessment of residual risk and uncertainty:

— Confidence levels for probability of failure and consequence severity for each failure mode/mechanism/cause should be defined and documented and may be marked on the company risk matrix.

The probability of failure, consequence severity, and technology risk should be assessed against requirements and risk acceptance criteria.

— Where requirements are not met, design changes and additional qualification activities may be required to improve reliability availability and integrity.

— If the potential risk exceeds acceptance criteria, additional actions should be identified to manage the risk and reduce it to an acceptable level. This may include additional inspection and monitoring as part of integrity management in operation or additional process checks and hold points.

The technology residual risk and uncertainties may be included in the qualification assurance document.

— Specific data used as evidence should be summarized in the qualification assurance report.

— Figure E.3 provides an example of a template that may be adapted to meet specific data recording purposes and for inclusion in the qualification assurance document.

E.4 TRL Descriptions

E.4.1 General

This section describes the meaning and intent of each TRL and provides a guide to the types of qualification activities that would typically be carried out at each TRL.

Each TRL is achieved by performing qualification activities that meet the functional and performance requirements specified by the customer. These requirements together with an understanding of failure modes, mechanisms, and causes are important in identifying specific qualification activities to be undertaken.

Sections E.4.2 to E.4.9 and Table E.3 provide guidance on the types of qualification action to be considered at each TRL from TRL 0 to TRL 7, respectively.

The generic TRL ladder described here should be reviewed and where necessary adapted into a technology-specific TRL ladder, with technology-specific expectations at each TRL stage.

Non Component Specific Template

Component / Assembly:	Component Description:		PQS #:	
Operator Governing Specification:			Rev#:	Date:
Supplier:	Supplier Component Identifier:	Ref. BOM#:	Ref. Assembly Drwg. #:	
OEM:				
Weight:	Dimensions (HxWxL):	TRL Number:	Ref. FMA#:	

Service Conditions	Required Operating Parameters	Supplier Design Rating

Qualifications - API or other existing Industry Practice

Performance Verification	Standard / Test Specification (inc. Rev. No.)	Supplier Test Procedure #	Supplier Comments / Deviations from Standards / Rev #	Scaled or Tested	Ref. Supplier Report #

Qualifications - Supplemental Practices (Optional)

Performance Verification	Standard / Test Specification (inc. Rev. No.)	Supplier Test Procedure #	Supplier Comments / Deviations from Standards / Rev #	Scaled or Tested	Ref. Supplier Report #

Interfaces

Description	Supplier Component Identifier	GA Drwg. #	Comments Regarding Stated Service and Functional Requirements

Additional Comments

Figure E.3—Sample Product Qualification Sheet

Table E.3—TRL Ladder Stages

TRL	Development Stage Completed
0	Basic Research (basic R&D, paper concept)
1	Concept Selection (proof of concept as a paper study or R&D experiment)
2	Concept Demonstration (experimental proof of concept using physical model tests)
3	Prototype Development (prototype functional, performance and reliability tested)
4	Product Validation (product validated and environment tested)
5	System Integration Testing (production system interface tested)
6	System Installation and Commissioning (production system installed and tested)
7	System Operation (production system field proven)

E.4.2 TRL 0—Basic Research

To achieve TRL 0, evidence should be created showing that the basic scientific or engineering principles have been observed and that there is an idea to exploit that principle in a novel piece of technology. This would likely take the form of a concept written down; there would likely be no analysis carried out to prove the idea, nor any historical data.

Conception activities to achieve TRL 0 should include:

— identify fundamental objectives and requirements;

— undertake R&D conceptual studies;

— sketch out basic form (shape, dimensions, etc.) and function;

— identify basic principles;

— back of the envelope type calculations;

— lessons learned review for similar technologies;

— identify key technical risks.

E.4.3 TRL 1—Concept Selection

To achieve TRL 1, evidence should be created to prove that the concept can be used in the desired application. This would take the form of low-level analysis, reference to features in common with existing technology, or basic R&D experimentation to prove the concept can function in the desired way.

For new technology, at this stage of development, it is generally expected that there will be no design or development history and that much of the work to achieve TRL 1 will take the form of paper studies without the need to develop physical models. However, some technologies, for example where the technology is dependent on experimentally observed phenomena, may require inclusion of R&D experimentation.

On completion of TRL 1 it is expected that the developer will have:

— formulated the technology concept and/or its potential applications;

— proven the concept and functionality through analysis or by reference to features common with existing technology.

To achieve TRL1, concept demonstration should include activities to:

— extend research to formulate concept and potential applications;

— formulate concept and demonstrate functionality by analysis;

— perform a preliminary assessment of fit (physical interfaces, etc.);

— prepare engineering drawings with some engineering calculations;

— review and update key technical risks.

E.4.4 TRL 2—Concept Demonstration

To achieve TRL 2, evidence should be created to demonstrate that the concept is valid. The evidence should be sufficient to prove that the technology has the potential to successfully function in its intended environment through material testing, engineering studies, and laboratory “mock-ups.”

For new technology at TRL 2 stage of development, it is generally expected that there is little or no design history and no environmental testing will have been carried out. During TRL 2, the focus should be on understanding and demonstrating functionality and materials requirements in preparation for construction of a prototype during TRL 3. Early reliability testing may also be performed on key parts or components in a testing laboratory ready for prototype construction.

TRL 2 concept demonstration work should include activities to:

— demonstrate functionality of the technology—physical models/lab “mock-up”;

— undertake initial FMECA;

— perform laboratory-scale material testing of degradation mechanisms;

— perform engineering studies to specify function/performance/reliability;

— identify reliability drivers;

— specify RAM requirements for technology overall/key components;

— review and update key technical risks.

E.4.5 TRL 3—Prototype Development

To achieve TRL 3, a prototype should be built and subjected to basic functional and reliability testing to build robustness and confidence into the functionality and performance of the new technology, together with its ability to perform for extended periods of time. At this stage the technology does not need to be integration into a broader system.

On completion of TRL 3 it is expected that the developer will have:

- built a prototype for testing. Prototype may be:
  - virtual or based;
  - software model of the system;
  - reduced scale;
- put the prototype through tests in relevant laboratory testing environments:
  - functional and performance tests;
  - reliability tests including: reliability growth tests;
  - highly accelerated life tests and accelerated life;
- built and run a number of component and system reliability prediction models for the technology;
- demonstrated the extent to which application requirements have been met together with potential benefits and risks.

TRL 3 prototype qualification testing should include activities to:

- visualize/demonstrate form, fit, and functional capability;
- perform detailed Q-FMECA;
- identify and perform any physical testing on the prototype in the factory or laboratory environment including:
  - RDT of function and performance requirements;
  - life testing;
  - ALT;
- identify and perform any required virtual prototype analysis/simulation;
- perform any required system reliability analyses;
- establish/confirm operating/destruct limits and degradation limits and degradation rates;
- address risks from the manufacture/assembly/transit/storage/installation;
- identify required in-service monitoring;
- estimate reliability and residual technical risks and uncertainty.

E.4.6 TRL 4—Product Validation

To achieve TRL 4, a prototype or first production unit should have been manufactured and assembled using the processes defined for the real production item. The product should have been subjected to testing in an environment equivalent to that of the environment in which it is designed to be used (e.g. hyperbaric testing), although it may not have been installed in its intended operating environment.

On completion of TRL 4 the developer should have:

- built the first full scale product of its type;
- put the product through environmental testing in a realistic environment;
- confirmed that functional and performance requirements are being met;
- updated component and system reliability prediction models for the technology;

— demonstrated the extent to which application requirements have been met together with potential benefits and risks;

TRL 4 environment qualification testing should typically include activities to:

— develop a specification for manufacture of production items;

— perform a P-FMECA for manufacture/assembly/transit/storage;

— establish a performance data collection system;

— perform product testing in simulated or actual subsea environment;

— confirm that degradation of function/performance within acceptable limits;

— verify acceptability of manufacturing/assembly process;

— perform stress screening to remove manufacture or assembly defects;

— estimate reliability and residual technical risks and uncertainty.

E.4.7 TRL 5—System Integration Testing

To achieve TRL 5, the final product to be deployed should be incorporated into its intended system. Full interface and function testing should be completed before it is placed in its intended environment. Particular focus should be given to the impact of the technology on the wider system reliability and integrity and the impact of the wider system on the technology reliability and integrity. At this stage there should be confidence that the item is ready to be installed as part of a field development project.

TRL 5 system qualification testing should include activities to:

— perform interface FMECA;

— perform function and performance tests when integrated with (connected to) the wider system, noting that SIT activities are not generally performed subsea;

— address mechanical, hydraulic, optical, electronic, software, ROV/tooling, and human interfaces;

— confirm product SIT requirements;

— initiate performance/reliability data collection;

— update system reliability assessment;

— estimate reliability and residual technical risks and uncertainty.

E.4.8 TRL 6—System Installation and Commissioning

During TRL 6, the technology will be installed and commissioned in its final operational environment and all required TRL 6 tests performed.

Qualification of an installed system to achieve TRL6 should include activities to:

— perform P-FMECA for installation/hook-up/commissioning;

— installation/hook-up/testing/commissioning with wider production system—not operating with production fluids;

— confirm product is able to work as intended/reliability not compromised by installation/hook-up/commissioning processes;

— update design FMECA;

— define detailed in-service inspection/monitoring/sampling;

— verify inspection/monitoring/sampling functionality;

— define preparedness response;

— complete interface/function qualification testing with reservoir hydrocarbons that could not be done before field start-up;

— identify remaining technical risks to be managed by operations.

E.4.9 TRL 7—System Operation

To achieve TRL 7, an item should be installed in the final operational environment, for sufficient duration to demonstrate acceptable reliability or availability performance. The length of time required to demonstrate field reliability performance will depend on the population of components and the failure rate of the equipment and will vary from system to system. Until that time is achieved the technology will not have progressed beyond TRL 6.

TRL 7 implies that the technology has demonstrated, with supporting evidence, the ability to function and perform reliably for the specified demonstration time for all scenarios encountered.

Typical qualification activities required for technology to achieve TRL7 include:

— implementation of in-service monitoring, sampling, and inspection;

— collection and analysis of reliability and integrity performance data;

— updating of FMECA with in-service performance data;

— undertaking RCFA for failed/underperforming items;

— implementing reliability improvements for failed/underperforming items,

— demonstrating that the technology functions in its operating environment with the required reliability for the required maintenance or failure-free operating period; this may be several years;

— feedback performance to projects/suppliers.

E.5 Guidance on Initial TRL for Modified Technology

E.5.1 General

Technology developments are most commonly modifications to, or extensions of, existing technology. This means that it is not always necessary for qualification programs to assume an initial TRL = 0.

Table E.4 provides guidance on initial TRL, given changes to a design, application, or specification together with key qualification activities that may be required. For example, if an existing package is required to meet a higher reliability or integrity specification, the package vendor may only be able to claim the technology has achieved TRL 2 and further qualification activities will be required to achieve TRL 3 and above.

It should be recognized that the guidance in Table E.4 is typical and conservative in that it represents the lowest initial TRL that is expected for a given change. If, within a particular application and context, a user decides to assign a higher initial TRL than that specified in Table E.4, this should be accompanied by evidence to justify the higher TRL.

Table E.4—Qualification of Existing Technology—Extensions and Modifications

Change	Minimum TRL Achieved	Example Qualification Actions
Technology	0 to 1	Identify any new failure modes and mechanisms. Estimate failure rates. Assess technical risk and uncertainty.
Function	0 to 1	Identify consequent modification/extension due to changed function. Identify any new failure modes and mechanisms. Estimate failure rates. Assess technical risk and uncertainty.
Reliability, integrity, durability, or life	2	Conduct robustness tests. Determine operating limits. Identify the system failure modes. Design for reliability.
Completely new material	0 to 1	Conduct further R&D activities. Conduct applicable materials testing.
System or assembly architecture	2 to 4	Identify any new failure modes and mechanisms. Estimate failure rates. Conduct robustness tests Identify system failure modes and consequences.
Subassembly or component design (shape, material, size, scale, etc.)	1 to 2	Identify any new failure modes and mechanisms. Estimate failure rates.
Software	No specific guidance	Obtain guidance and recommendations on initial software TRL from software specialists, subsea technical authority, or industry experts.
Manufacture, assembly, or construction process	2 to 3	Conduct process FMECA to determine impact of change to manufacture on equipment reliability.
Loading	2	Identify loading (static, dynamic, shock). Assess combined loading and load limits. Assess load affected deterioration/damage accumulation. Conduct stress tests and FEA.
Pressure and temperature (internal and external) Environment (chemical—internal and external)	2	Identify any new failure modes and mechanisms. Estimate failure rates. Assess operating limits. Conduct sensitivity analysis

E.5.2 Alternative TRL 1 to 9 Ladders

It is recognized that some organizations and other industries use alternative TRL ladders; many of these are based on a TRL 1 to TRL 9 system that evolved from the original NASA TRL ladder.

If an alternative ladder is used, then all parties involved in the technology qualification should agree on the TRL ladder to be used with clear definitions of each level.

Further guidance on different TRL ladders will be provided in the Second Edition of API 17Q currently under development.

Annex F
(informative)

Application of Test Statistics

NOTE This annex is included to provide interim guidance until the next edition of API 17Q is published and may be removed at that time. The next edition of API 17Q is completely rewritten from the First Edition, providing more detailed guidance for the industry on new technology qualification including qualification of modified/extended technology.

F.1 General

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.)

F.2 Application of Test Statistics of Continuous Operation Components

F.2.1 General

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 References [24] and [25].

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 (see note)];

— estimating the reliability parameters (e.g. the MTTF).

NOTE The minimum number of tests to failure to indicate that the pattern has a constant hazard rate is 4, but ideally, for greater confidence, a larger population is typically used.

Table F.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 F.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	0.0557	8	1.4327	15	2.3845
2	0.1286	9	1.6348	16	3.1419
3	0.3020	10	1.6481	17	3.2536
4	0.3281	11	1.7708	18	3.6551
5	0.5329	12	1.8526	19	4.2949
6	0.8030	13	1.8544	20	7.8356
7	0.9877	14	1.8974		

F.2.2 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 ith failure as:

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

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

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

where

n is the number of samples in the test;

t_i is the time of the ith failure;

t_r is the time of the last (rth) failure;

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

NOTE where $n = r$, $T_r = T^*$.

Table F.2 gives T_i values for this example

Table F.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	1.1140	8	21.7631	15	29.5358
2	2.4991	9	24.1883	16	33.3228
3	5.6203	10	24.3346	17	33.7696
4	6.0640	11	25.5616	18	34.9741
5	9.3408	12	26.2978	19	36.2537
6	13.3923	13	26.3122	20	39.7944
7	15.9781	14	26.6132		

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

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

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, $X^2(v)$, where $v = 2d$.

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

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

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

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

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

In this example, $X^2_{0.95}(38) > 35.52 > X^2_{0.05}(38)$; 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.

F.2.3 Estimating the Failure Parameter

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

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

$$\hat{\lambda} = \frac{r}{T^*} \tag{F.4}$$

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:

$$\lambda_{L2} = \frac{X^2_{\alpha/2}(2r)}{2T^*} \tag{F.5}$$

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

$$\lambda_{U2} = \frac{X^2_{1-\alpha/2}(2r)}{2T^*} \tag{F.6}$$

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

$$\hat{\lambda} = \frac{20}{39.79} \approx 0.5 \tag{F.7}$$

This corresponds to an MTTF 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:

$$\lambda_{L2} = \frac{X^2_{\alpha/2}(2r)}{2T^*} = \frac{X^2_{0.05}(20)}{79.58} = \frac{26.51}{79.58} = 0.33 \tag{F.8}$$

which corresponds to an MTTF of 3 years; the upper limit is calculated as:

$$\lambda_{L2} = \frac{X^2_{1-\alpha/2}(2r)}{2T^*} = \frac{X^2_{0.95}(20)}{79.58} = \frac{55.76}{79.58} = 0.69 \tag{F.9}$$

This corresponds to an MTTF of 1.45 years.

F.3 Application of Test Statistics for Noncontinuous Operation

F.3.1 General

Performance verification of equipment is often drawn from API 6A and API 17D cycle test requirements, intended to validate noncontinuous 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, the following calculation method may be used to estimate MTBF until proper field data become available. The chi-square distribution (X^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:

$$\text{lower limit}_{\text{cycles}} = \frac{2T_{(\text{cycles})}}{X^2_{(2r+2,\,\alpha)}} \tag{F.10}$$

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 – α) is the lower confidence factor of the MTBF;

(e.g. 50 % confidence $\rightarrow$ α = 0.5; 30 % confidence $\rightarrow$ α = 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 X^2, $(2r + 2)$ is referred to as the degree of freedom variable, and α is referred to as the noncentrality function.

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

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:

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

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 are typically made explicit.

F.3.2 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.

Table F.3—Chi-squared Distribution Table

Confidence Factor P_x (1 – α)	α	X^2 (2r + 2, α)		
		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 X^2 function and its estimated MTBF when predicting reliability for performance verification tests found in API 17D or API 6A.

F.3.3 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:

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

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

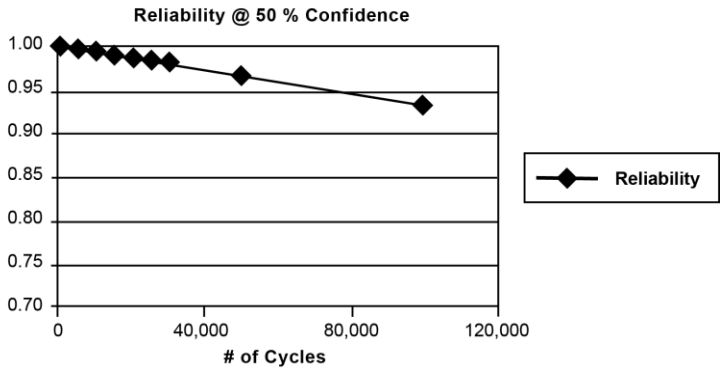
$$\text{MTBF}_{(\text{cycles})} = 1{,}443{,}000 \tag{F.13}$$

Applying the exponential reliability equation:

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

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:

$$\text{MTBF}_{(\text{years})} = 1{,}443{,}000/500 = 2{,}886 \text{ years} \tag{F.15}$$

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:

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

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

$$MTBF_{(cycles)} = 431 \tag{F.17}$$

Assuming that the valve performs 12 cycles per year:

$$MTBF_{(years)} = 431/12 = 35.9 \text{ years} \tag{F.18}$$

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 API 17Q.

Bibliography

[1] API Standard 18LCM, *Standard for Product Life Cycle Management*, First Edition

[2] ISO 31000, *Risk management—Principles and guidelines*, 2009

[3] API Publication 770, *Manager's Guide to Reducing Human Errors Improving Human Performance in the Process Industries*, 2001

[4] ISO 10007, *Quality management systems—Guidelines for configuration management*, 2003

[5] MIL-HDBK-61 A, *Configuration Management Guidance*, 2001

[6] SAE EIA-649B, *Configuration Management Standard*, 2011

[7] A.D.S. Carter, *Mechanical Reliability*, Macmillan, 1972

[8] IEC 60812, *Analysis techniques for system reliability—Procedure for failure mode and effects analysis (FMEA)*, 2006

[9] BS EN 61025:2007*, Fault tree analysis (FTA)*, 2007

[10] BS EN 61078:2006, *Analysis techniques for dependability—Reliability block diagram and boolean methods*, 2006

[11] R.N. Allan and R. Billinton, *Reliability Evaluation of Engineering Systems: Concepts and Techniques*, Second Edition, 1992

[12] R.E. Melchers, *Structural Reliability: Analysis and Prediction*, 1999

[13] D. Kececioglu, *Robust Engineering Design-By-Reliability with Emphasis on Mechanical Components and Structural Reliability*, DEStech Publications, 2003

[14] S. Stephenson, T. McCoy, and J. Thomas, “Do You Have Enough Strength to Take the Stress?,” *Proceedings of the International Applied Reliability Symposium*, 2005

[15] T. Bedford and R. Cooke, *Probablistic Risk Analysis: Foundations and Methods*, Cambridge University Press, 2001

[16] C. Sundararajan, *Guide to Reliability Engineering: Data, Analysis, Applications, Implementation, and Management*, Van Nostrand, 1991

[17] R.K. Mobley, *Root Cause Failure Analysis*, Butterworth-Heinemann, 1999

[18] B. Tyler, F. Crawley, and M. Preston, *HAZOP: Guide to Best Practice*, IChemE, Second Edition, 2008

[19] IEC 61882, *Hazard and operability studies (HAZOP studies)—Application guide*, 2001

[20] BS EN ISO 17776:2002, *Petroleum and natural gas industries—Offshore production installations. Guidance on tools and techniques for hazard identification and risk assessment*, 2001

[21] ISO 31010:2009, *Risk management—Risk assessment techniques*, 2009

[22] J.E. Strutt, J.V. Sharp, E. Terry, and R. Miles, “Capability Maturity Models for Offshore Organisational Management,” *Environment International,* 2006

[23] J.V. Sharp, J.E. Strutt, J. Busby, and E. Terry, “Measurement of Organisational Maturity in Designing Safe Offshore Installations,” *OMAE*, 2002

[24] P.P. O'Connor and A. Kleyner, *Practical Reliability Engineering*, Fourth Edition, Wiley, 2002

[25] IEC 61164:2004, *Reliability growth—Statistical test and estimation methods*, 2004

[26] BS 6079-1:2010, *Project management—Part 1: Principles and guidelines for the management of projects*

[27] API Specification Q1, *Specification for Quality Management System Requirements for Manufacturing Organizations for the Petroleum and Natural Gas Industry,* Ninth Edition, June 2013

[28] API Specification Q2, *Specification for Quality Management System Requirements for Service Supply Organizations for the Petroleum and Natural Gas Industries*, First Edition, December 2011

[29] Energy Institute, *Guidelines for the management of integrity of subsea facilities*

[30] API Specification 6A, *Specification for Wellhead and Christmas Tree Equipment*, Twentieth Edition, October 2012

[31] API Specification 17D, *Specification for Subsea Wellhead and Christmas Tree Equipment*, Second Edition, July 2016

AMERICAN PETROLEUM INSTITUTE

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

202-682-8000

Additional copies are available online at www.api.org/pubs

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	

Information about API publications, programs and services is available on the web at www.api.org.

Product No. G17N02