Guidelines for Reliability, Maintainability and Survivability of Marine Energy Conversion Systems

Foreword

This document has been prepared in consultation with The European Marine Energy Centre Ltd (EMEC) and with other interested parties in the UK marine energy community. It is one of twelve publications in the *Marine Renewable Energy Guides* series, included in the following figure.

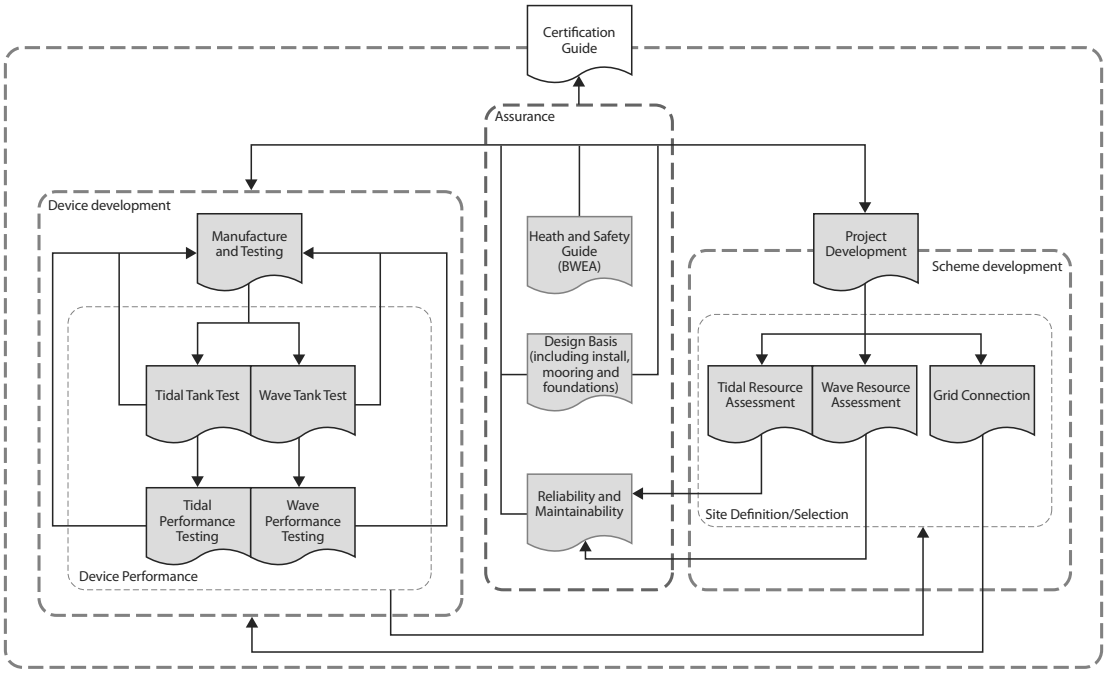

Figure 1 — Marine Renewable Energy Guides

Acknowledgements

This document had been produced by Michael Starling of BMT Cordah Ltd under a contract from the European Marine Energy Centre. It is based on extensive stakeholder consultations at a number of workshops.

Peer Review has been carried out with Professor J. V. Sharp, Cranfield University.

Guidelines for Reliability, Maintainability and Survivability of Marine Energy Conversion Systems

Marine Renewable Energy Guides

EMEC ORKNEY™
The European Marine Energy Centre Ltd

First published in the UK in 2009 by BSI, 389 Chiswick High Road, London W4 4AL

Typeset in Great Britain by Monolith – www.monolith.uk.com
Printed by The Charlesworth Group, Wakefield

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

ISBN 978-0-580-65362-9

Contents

Guidelines for Reliability, Maintainability and Survivability of Marine Energy Conversion Systems

Introduction

The purpose of this guide is to help promote the development of a successful energy generation industry based on the widespread manufacture and deployment of reliable marine energy converters.

The guide is flexible, in that it does not prescribe a set way of doing things, but outlines a range of techniques that can be used.

The guidance is goal-based, in that it takes as its starting point the definitions of the reliability, maintainability and survivability requirements for a successful and economic energy farm and applies these requirements to the individual converter and suggests tools and techniques to help meet these requirements.

This document focuses on three areas that are of fundamental importance to the success of a marine energy conversion system; they should be considered at all stages from concept to production. These are:

- **reliability**, and in particular the trade-offs between component reliability and system redundancy to achieve the required availability;
- **maintainability**, and in particular the methods of, and access for, preventive and corrective maintenance;
- **survivability**, and in particular the opportunities for avoiding extreme loadings and conditions.

Status of the industry

This document recognizes that the industry is in its infancy and so it has been drafted to ensure that its application can be flexible and beneficial to concept designs, prototypes under development, pre-production installations, and experimental marine energy farms, as well as to small-scale and large-scale commercial applications.

Application

Typical application of this document may include the following:

- **At all stages** – to make sure that the requirements for reliability, maintainability and survivability for a deployed energy farm are identified and are deconstructed into marine energy converter level requirements;
- **Concept stage** – to make sure that there are not any long-term reliability, maintainability and survivability risks that cannot be resolved during the project development;
- **Prototype stage** – to avoid critical failures that can discourage investors or give the product/process a bad name;
- **Pre-production stage** – to design in reliability, maintainability and survivability;
- **Energy farm stage** – to build converter level reliability, maintainability and survivability performance (and predictions) into an estimation of performance of the deployed energy farm.

Users

This document is intended for use by marine energy converter developers to demonstrate and improve their converters, project developers to evaluate their projects and investors to ensure due diligence on their decisions.

The main clauses of the guide, and the typical outputs, are shown in Figure 2.

1 Scope

It is intended that this guidance document can be used to improve and/or demonstrate the reliability, maintainability and survivability of marine energy converters that extract energy from waves and from tides and tidal streams.

It is not intended to apply to tidal barrages or tidal lagoons.

2 Normative references

The following referenced document is indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60050 – 191, *International electrotechnical vocabulary (IEV) – Part 191: Dependability and quality of service*

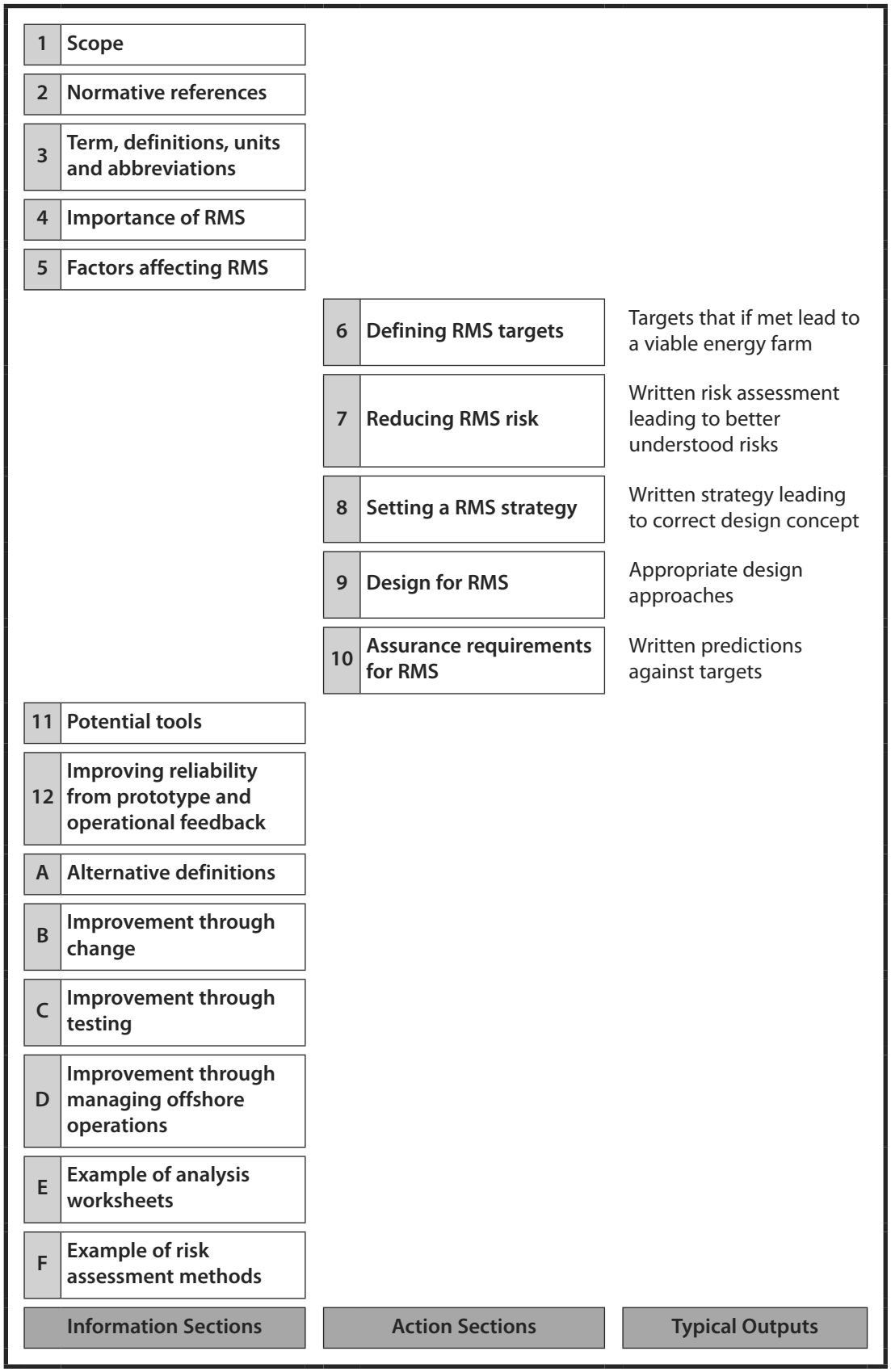

Figure 2 — Main clauses of the guide

3 Terms, definitions, units and abbreviations

For the purposes of this document, the following terms, definitions, units and abbreviations apply.

3.1 Terms and definitions

3.1.1
reliability
probability that an item can perform a required function under given conditions for a given time interval [IEC 60050 – 191-12-01]

3.1.2
maintainability
probability that a given active maintenance action, for an item under given conditions of use, can be carried out within a stated time interval, when the maintenance is performed under stated conditions and using stated procedures and resources [IEC 60050-191-13-01]

3.1.3
availability
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 [IEC 60050-191- 02-05]

NOTE For continuously running equipment this equates to:

$$\frac{\text{uptime}}{\text{uptime} + \text{downtime}}$$

Where reliability is specified in Mean Time Between Failures (MTBF) and maintainability in Mean Time To Repair (MTTR) this also equates to:

$$\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

3.1.4
survivability

3.1.4.1
safety survivability
probability that the converter will stay on station over the stated operational life

NOTE This could be 25 years, for example

3.1.4.2
functional survivability
probability that the converter will produce its rated energy (or an allowed degraded energy rating) without damage leading to the need for major unplanned removal or repair over the stated operational life

NOTE 1 Issues to consider when considering survivability include the ability to survive discrete events such as major storms, peak waves and the ability to survive long-term conditions such as the cumulative battering of the waves, the long-term corrosion effects and fatigue and other wear out processes

NOTE 2 This definition refers to the survivability of the converter. Care will need to be taken when scaling this to the survivability of a power station made up of multiple converters as some of the issues are common mode issues, for example, a peak wave passing across all the converters, and others are not.

3.1.5
marine energy converter
energy extraction and generation device, the moorings and/or foundations and cabling and other connections

3.2 Units and abbreviations

3.2.1 Capacity factor

The capacity factor of the marine energy converter is the ratio of the average power generated during a year by a fully functional converter to the peak power that can be generated

NOTE 1 The amount of energy generated should be given in kilowatt-hours (KWh) or as appropriate megawatt-hours (MWh), gigawatt-hours (GWh), terawatt-hours (TWh), etc.

NOTE 2 The amount of power generated should be given in kilowatts (KW) or as appropriate megawatts (MW), gigawatts (GW), etc.

3.2.2 Abbreviations

BSI	British Standards Institution
CapEx	Capital Expenditure
DRACAS	Data Reporting And Corrective Action System
FEED	Front End Engineering Design
FFOP	Failure Free Operating Period
FMECA	Failure Modes Effects and Criticality Analysis
FRACAS	Failure Reporting And Corrective Action System
HAZOP Study	Hazard and Operability Study
IEC	International Electrotechnical Commission
MFOP	Maintenance Free Operating Period
MRP	Maintenance Recovery Period
MTA	Maintenance Task Analysis
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
OpEx	Operational Expenditure

RCM	Reliability-centred Maintenance
RiskEx	Risk Expenditure
RMS	Reliability, Maintainability, Survivability

4 Importance of reliability, maintainability and survivability

Reliability, maintainability and survivability are crucial to the economic and environmental case for a marine energy converter. These factors affect Capital Expenditure (CapEx), Revenue, Operational Expenditure (OpEx) and Risk Expenditure (RiskEx) and would entail the following considerations:

CapEx

- the design of the equipment;
- the supply chain for the equipment;
- the installation of the equipment.

Revenue

- the environment in which the converter can be installed and operated;
- the energy generated by the converters and hence the revenue to the project.

OpEx

- the amount of maintenance required;
- the cost of maintenance of the converters.

RiskEx

- the ability to raise investment and the cost of the investment;
- the ability to insure and certify and the cost of insurance;
- the effect on the asset/safety/environment of failure and the cost to rectify;
- warranty costs.

5 Factors affecting reliability, maintainability and survivability

5.1 Technical and operational factors

There are numerous technical and operational factors that affect reliability, maintainability and survivability. This clause provides a checklist of the main ones that may apply.

Technical factors	
Energy farm configuration	Number of converters
	Location of converters
	Number of offshore sub-stations
	Offshore cable architecture (inter-array and export cables)
	Onshore cable architecture to grid connection point
Converter reliability	Failure rate of equipment and systems
	Effect of failure on generation
	Required repair action
Maintenance and repair policy	Balance between preventive, corrective and on-condition maintenance
	Maintenance task frequency
	Maintenance task duration
	Access to converter for maintenance
	Required resources for maintenance

Operational factors	
Accessibility	Necessary metocean conditions for installation and for maintenance
Ability to work on converters	Method for getting staff to and from the converter
	Method for getting staff on and off the converter
	Methods for staff to safely and effectively work on the converter
Ability to remove the converter	Method of disconnecting the converter

	Method for taking the converter off-station
	Methods for working on the converter off-station
	Method for putting the converter back on station
	Method for re-connecting the converter
Metocean conditions	Wind speed and direction
	Wave height, period and direction
	Tidal current velocity
	Tidal periods
	Water depth
	Daylight and visibility
	Sea ice
	Threat of storms
Environmental conditions	Temperature
	Rain
	Lightning
Ability to generate during failures or maintenance	Ability to defer failures by reducing operating conditions to slack or calm water
	Ability to defer maintenance to slack or calm water
	Duration of slack water for maintenance
	Duration of calm water for maintenance
Marine resources required	The types and numbers of vessels required
	The location of the vessels
	The transit times from shore bases
	The capability of the vessels
	The availability of relevant personnel with appropriate expertise

5.2 Weather factors

5.2.1 General

Weather and metocean conditions are important to all aspects of marine energy converter design, performance and operation and it is therefore important to have a

good understanding of how generic converter capability is affected by site-specific factors and to do this, good quality data is required from verifiable data sources.

5.2.2 Recommendations for metocean data

5.2.2.1 Near-shore effects

Many sites considered for converters are near-shore or are in areas of shallow water. Most metocean data are derived from hindcast models that are well-suited to deep, open waters well away from land. Near-shore and shallow-water corrections should be considered before such data are used to represent the site in question. Date on wave loading through the water column during severe storms is of particular importance as is the turbulence of the flow.

In addition, local knowledge should be sought regarding local effects that may not appear in large-area data sets.

5.2.2.2 Need for correlated data

Installation and maintenance operations at sea require 'weather windows'. These are defined by the ability of personnel to transit to and access the converter and the ability of the vessels required to carry out the operations.

This weather window is based on a variety of factors including, for example, wind, waves, current, visibility, light and therefore it is important that the metocean data are either in the form of a correlated time history or, if this is not available, they should be in the form of a probability distribution of weather windows.

5.3 Combining technical and operational factors with weather factors

The effects of these factors are a combination of those generic to the machines (e.g. for energy generation) and others specific to its location (e.g. access constraints). It is important to have a correlation between parameters affecting reliability and access with those affecting energy generation.

6 Defining reliability, maintainability and survivability targets

6.1 General

This guide is aimed at all types of wave and tidal devices and therefore it is not appropriate to specify a particular way of setting targets; instead it describes the principles to be considered in setting targets.

6.2 Availability target

Marine energy converters are generally anticipated to be used in farms with multiple converters. The availability requirements for the converter flow from the fundamental business case for the project. This is likely to result in two key parameters:

- the required availability;
- the operating cost for achieving the availability.

An availability target should be set for:

- the energy farm as a whole;
- each converter within the farm.

The basis of the availability target, and how the availability targets links to the revenue generation requirement, should be clearly defined.

6.3 Reliability and maintainability targets

6.3.1 Traditional methods for specifying converter reliability and maintainability

The traditional method for specifying reliability and maintainability is by:

- mean time between failures (MTBF);
- mean time to repair (MTTR).

In the context of marine energy converters, it is unlikely that these measures can be derived from energy farm requirements or known converter achievement extrapolated into expected energy farm performance.

6.3.2 Alternative methods for specifying converter reliability and maintainability

Where the ability to maintain a converter is constrained by time (e.g. a summer maintenance season or to coincide with the availability of a boat) an alternative way of specifying converter reliability is by:

- maintenance free operating periods (MFOP) – the length of time the equipment is expected to operate without maintenance, e.g. 20 years for a foundation, 1 year for a service;
- maintenance recovery period (MRP) – the length of time, after the maintenance free operating period, to bring the equipment up to a state where the maintenance free operating period can be restarted, e.g. a single slack water period;

- allowable degraded performance – the drop in performance allowable between maintenance, e.g. making the failed state still capable of generating energy, but at a reduced rate;
- maximum probability of premature failure – the probability it will fail before the end of its maintenance free operating period.

6.3.3 Survivability target

The survivability targets for both safety and functionality should be set for:

- the energy farm as a whole;
- each converter within the farm.

The basis of the survivability target, and how the survivability targets link to the business case, the environmental impact of failures, and the safety justifications should be clearly defined.

It is particularly important to note that survivability issues may be common mode, i.e. a single event can threaten the survivability of all the converters in an energy farm at the same time.

6.3.4 Typical output – written targets

The targets should be written, initially as part of the design, but kept up-to-date, and be made widely available.

7 Reducing reliability, maintainability and survivability risk

7.1 General

Reliability, maintainability and survivability are features of a design that are competing for development and test resources. One of the methods for deciding the relative priorities for resource allocation is to assess the level of technical risk of the various components of the converter. This assessment can be used to:

- target areas for risk reduction activities;
- set factors of safety to mitigate risk;
- set levels of contingency to be used should risks materialize.

7.2 Scalability of the risk assessment methods

These approaches need to be scalable in that they can be applied to:

- the totality of the applied technology as well as each separate part, function and subsystem;
- each organization involved in the design, build operations and maintenance.

7.3 Typical output – written risk assessment

The risk assessment should be written, initially as part of the design, but kept up-to-date, and include as a minimum:

- success criteria;
- overview of the design;
- main risk areas;
- risk identification, analysis and control;
- response to the risks.

8 Setting a reliability, maintainability and survivability strategy

8.1 General

The reliability, maintainability and survivability strategy should be well thought through and clearly defined. There are numerous trade-offs that are required including:

- the balance between reliability and maintainability;
- the balance between reliability and redundancy;
- the incorporation, or not, of avoidance features.

8.2 Balance between reliability and maintainability

The ideal is high reliability and good maintainability, but this may not be technically feasible or economically justifiable. In practice there is a balance between reliability and maintainability, for example, when selecting a design concept the same level of availability may be achieved by:

- high reliability and poor maintainability;

or

- good maintainability and low reliability.

8.3 Balance between reliability and redundancy

The choice between investment in high component reliability and redundancy needs to be made at the design stage, for example, when selecting a design concept the same level of reliability may be achieved by:

- high component reliability and low redundancy;

or

- high redundancy and low component reliability.

It is important to note that redundancy in situations where maintenance cannot be done, or can only be done after a significant length of time, may not greatly improve the overall reliability of equipment. The result may only be more failed equipment.

8.4 Incorporation of avoidance features

When selecting a design concept the same level of survivability may be achieved by:

- high factors of safety and a fixed installation;

or

- lower factors of safety and a reliable means of taking avoidance actions, such as minimizing loads, moving out of harm's way, moving into shelter.

8.5 Typical output – written reliability, maintainability and survivability strategy

The strategy should be written, initially as part of the design, but kept up to date and include as a minimum:

- an installation plan;
- an operations plan;
- an inspection plan;
- a preventive maintenance plan;
- a corrective maintenance plan.

9 Design for reliability, maintainability and survivability

The marine energy converter business is in its infancy and applying mature industry process to it is likely to be financially difficult, however, it is possible to recommend some key processes that should be followed:

- Requirements definition – defining and managing reliability objectives/targets during the design stage and the specification of these objectives/targets on suppliers and sub-suppliers;
- Reliability improvement – data collection, reliability analysis and improvement during design;
- Performance monitoring – collecting and correlating converter performance with operational circumstances;
- Design for ease and affordable cost of maintenance – design of maintenance and recovery systems to be based on accessibility for maintenance.

It is recommended this process is followed under the overarching process of reliability assurance and using the concept of the reliability case. This is described in Clause 10.

It is also recommended that formal tools, such as failure modes effects and criticality analysis are used. A range of tools are described in Clause 11.

The use of assurance and formal tools does not, in itself, improve reliability, maintainability and survivability. Improvement is made through change and some of the areas where change can be made are listed in Annex B.

10 Assurance requirements for reliability, maintainability and survivability

10.1 General

The recommended process for reliability assurance is to:

- follow a defined assurance process;
- present the results as a reliability case.

10.2 Typical assurance process

The fundamentals of an assurance process are simple. They are:

- to **define** what the equipment has to do;
- to **design** it and operate it to do it;

- to find some **evidence** that it will work and keep on working;
- identify and eliminate **threats** to success.

This is an iterative process as shown in Figure 3 below.

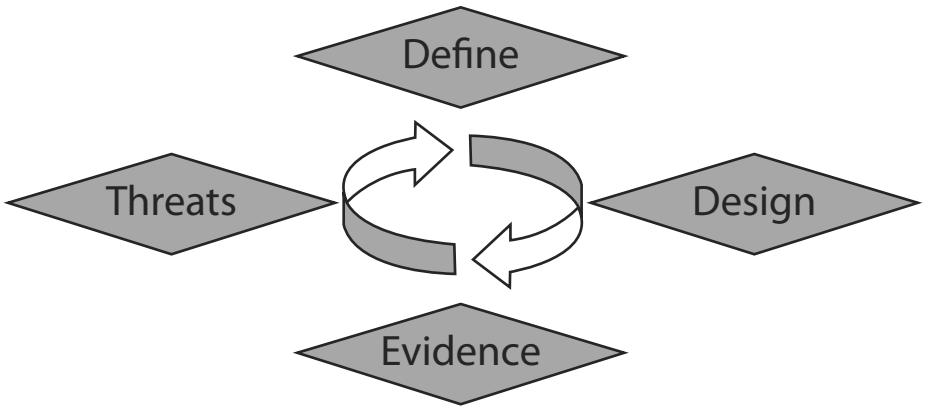

Figure 3 — Typical iterative reliability assurance process

10.3 Typical assurance tools

The typical tools that are central to assurance are:

- failure modes, effects and criticality analysis (FMECA) – which analyses what can go wrong technically;
- hazard and operability studies (HAZOP) – which analyses what can go wrong operationally;
- maintenance task analysis (MTA) – which analyses what actions and resources are required.

These are described in more detail in Clause 11.

10.4 Typical assurance methodology

The methodology of choice for success-based reliability assurance is the reliability case, the new progressive assurance technique for achieving high reliability and ease of maintenance that has been developed by the military and is being adopted by other industries.

The benefits of building a reliability case is that:

- reliability is improved through understanding what is required to make the system work reliably and therefore being able to make changes that maximizes reliability;

- improvement can be obtained quickly due to the ability to tailor the process to the problem.

The process can be summarized as cycles of interlinked activities including:

- producing reliability requirements matched to the operational and financial requirements;
- seeking evidence that requirements will be met;
- identifying reliability risks and assessing the level of risk;
- making a claim of reliability performance and the risk associated with the claim based on the evidence;
- taking action to build evidence and reduce risk;

leading to a 'claim of expected performance' and the 'risk associated with the claim' published in a reliability case report that is scrutinized by the management process.

10.5 Evidence in support

Reliability assurance is built from evidence. This evidence can be thought of as:

- evidence of success, i.e. evidence that is supportive of the claim that the reliability, maintainability and survivability targets will be met;
- evidence of failure, i.e. evidence that challenges the claim that the reliability, maintainability and survivability targets will be met.

With evidence of success the challenge is to prove that this evidence is relevant and applicable.

With evidence of failure the challenge is to prove that the evidence is not relevant or that specific steps have been taken that make it no longer applicable.

Reliability assurance should be centred on finding evidence of success. At the start of the process it should be assumed that there is 'no evidence that the system or process will work' and to find evidence to 'show that it will work'.

10.5.1 Assessing the quality of the evidence

The quality of the evidence is crucial, a reliability case can be thought of as a legal case, one item of incorrect evidence can bring the whole case down.

Evidence quality needs to be formally assessed. Current in-service operation and trials are examples of the best evidence (which is the closest that can be got to proving reliability) and no evidence and verbal expert opinion are examples of the worst evidence (where the reliability is only based on faith). In practice much evidence is between these two extremes and has to be used with care.

Good evidence does not automatically lead to good reliability as there may be excellent evidence that supports bad reliability. It is important that all the evidence found is used, evidence supporting reliability and evidence challenging it.

An example of a formal evidence categorization system used is shown in Figure 4.

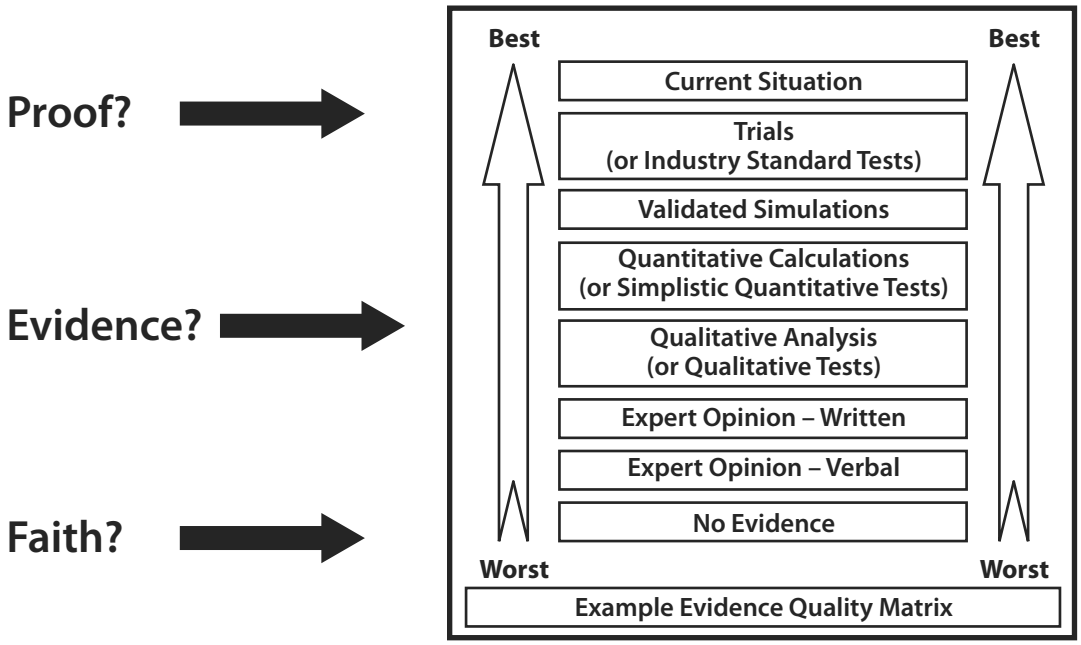

Figure 4 — Evidence quality categorization

10.5.2 Assessing the relevance and applicability of the evidence

Obtaining and scrutinizing evidence is crucial to reliability. Particular emphasis needs to be placed on:

- the origin of the evidence to make sure it is relevant to the reliability case;
- the aspects of the installation, design and operation the evidence is being used to support;
- an assessment of the evidence together with a formal categorization of its quality;
- the importance of the evidence to the reliability justification;
- the actions required to obtain more evidence;
- recording the build-up of evidence in an evidence register so it can be scrutinized;
- the effect of new evidence bringing unexpected results;
- responsibilities for obtaining evidence so that it is obtained and not forgotten;
- the effect of evidence being proved wrong.

10.6 Sources of evidence

There are numerous sources of evidence, however, most evidence falls into two categories, external and internal.

External evidence is essentially evidence that is out of the control of the converter design process. It includes evidence such as:

- third-party reports;
- data from other systems;
- publicly available data.

Internal evidence is evidence that is in the control of the converter design process. It includes data such as:

- development testing;
- prototype testing;
- production testing;
- commissioning;
- in-service data.

There are numerous methods of recording and analysing these types of data and in particular for analysing in-service data. The following have been identified as particularly relevant when analysing in-service data in ISO 20815 *Petroleum, petrochemical and natural gas industries*.

Relevance of the equipment

- the data should originate from the same type of equipment
- the data should originate from equipment using similar technology
- the data should originate from identical equipment models

Relevance of the operation

- the data should originate from periods of stable operation (although start-up problems should be given due consideration)
- the data should, if possible, originate from equipment which has been exposed to comparable operating and maintenance conditions

Statistical significance

- the basis for the data should be sufficiently extensive
- the amount of inventories and failure events used to predict reliability parameters should be sufficiently large to avoid bias resulting from 'outliers'
- population data (e.g. operating time, observation period) should be indicated to reflect statistical significance

Data sources

- the repair and downtime data should reflect site specific conditions
- the equipment boundary for originating data source and analysis element should match as far as possible. Study assumptions should otherwise be given
- data sources should be quoted.

10.7 Design review

The design should be reviewed periodically during the project. This review may include:

- internal design reviews;
- external design reviews;
- third-party validation;
- due diligence reviews.

10.8 Prediction against targets

An important part of assurance is to produce predictions against the reliability, maintainability and survivability targets set. There are a range of methods that can be used ranging from spreadsheet calculations, reliability modelling (e.g. reliability block diagrams) to system simulations.

Whatever method is used it is important that:

- the assessment methods and modelling tools have been verified;[1]
- the results have been validated.[2]

10.9 Typical outputs – written prediction against targets with supporting justifications

The prediction against targets should be written, initially as part of the design but kept current, and be made widely available.

It should form part of a reliability case report.

---

[1] Verification: Confirmation through the provision of objective evidence that specified requirements have been fulfilled. In software development, verification is the process of evaluating the (software) products of a given phase, or segment of work, to ensure correctness and consistency with respect to the products and standards provided as input to that stage. (ISO 9000:2000 TickIT guide)

[2] Validation: Confirmation through the provision of objective evidence that the requirements for a specific intended use or application have been fulfilled. (ISO 9000:2000 TickIT guide)

11 Potential tools

11.1 General

There are a large number of tools that are available to improve reliability and this document does not attempt to list them all. Instead it lists some of the principal tools and the benefits from using them. These are:

Tool	Uses	Link to other techniques
Failure Modes Effects and Criticality Analysis	Identifying what can go wrong technically and how to: • prevent it (e.g. design change). • react to it (e.g. identifying what maintenance or repair action is required).	FMECA analysis can be an important input into safety studies.
Hazard and Operability Study	Identifying what can go wrong operationally and how to: • prevent it (e.g. procedural change) • react to it (e.g. contingency plans).	HAZOP studies are often done as part of a safety study. Provided the HAZOP is correctly structured a reliability HAZOP can be used for safety and vice versa.
Maintenance Task Analysis	Identifying what actions and resources are required for: • keeping equipment in the required state (preventive maintenance) • reacting to failure (corrective maintenance) • reacting to measurements (on-condition or predictive maintenance	Getting the correct balance between preventive, corrective and predictive maintenance can be addressed by reliability-centred maintenance (RCM techniques).

11.2 Failure modes effects and criticality analysis

A failure modes effects and criticality analysis is a procedure where each potential failure mode of a component, equipment or subsystem in a system is analysed to determine the results of effects on the overall system and to classify each potential failure mode according to its probability and severity.

FMECA can be done in two ways. It can be:

- an analyst-based process where an analyst works on their own with the technical information and fills in the FMECA worksheets;
- a meeting-based process where a team is brought together with a chair and a recorder and the worksheets are developed by the team.

FMECA are typically done as an analyst-based process.

11.3 Hazard and operability studies

HAZOPs were originally developed for use at manufacturing facilities such as oil refineries, offshore oil platforms, petrochemical and chemical plants, natural gas processing plants and power plants, but its application has expanded.

A HAZOP study is a systematic method for examining complex facilities or processes to find actual or potentially hazardous procedures and operations so that they may be eliminated or mitigated. HAZOP studies are performed by a team consisting of plant operators, engineers, managers and others, some of whom should be intimately familiar with the facility being studied.

A HAZOP uses guide words (e.g. 'more', 'less', 'as well as') and parameters (e.g. 'temperature', 'control', 'ventilation') to consider process intent, possible deviations from the intended process, the consequences of any deviations, and the hazards presented by these consequences.

Although originally developed for analysing safety, it can also be applied to reliability analysis.

HAZOPs can also be done in two ways. It can be an analyst-based process or a meeting-based process.

HAZOPs are usually done as a meeting-based process.

11.4 Maintenance task analysis

A maintenance task analysis is a systematic way of analysing the maintenance requirements for a design. The purpose is to identify the resources, parts and consumables required, the environmental conditions that are required for the maintenance activity, the duration of the maintenance and the ability of the generator to continue generating during maintenance.

12 Improving reliability from prototype and operational feedback

12.1 General

There are also a large number of tools that are available to manage prototype and operational feedback and this guide is not in a position to list them all, however, instead it lists some of the principal tools and the benefits from using them. These are:

Tool	Uses	Link to other techniques
Failure Reporting And Corrective Action System (FRACAS)	To collect data on failures for analysis and action.	FRACAS systems may be a necessary part of a safety management system.
Data Recording And Corrective Action System (DRACAS)	To collect a wider range of data for analysis and action.	DRACAS systems may be a necessary part of a safety management system.
Lessons Learned	To identify from a problem its root cause, the lesson learned and where that lesson has to be applied.	

12.2 Failure reporting and corrective action system

A FRACAS is a closed loop activity that records and collates information in a database that enables product weaknesses to be identified, the causes analysed, and for appropriate corrective action to be implemented and managed.

To ensure that the FRACAS activity is as effective as possible, it should be readily available to everyone and should be as self-explanatory as possible with an integral training and help package. To improve the ease with which a FRACAS database can be interrogated the events should be categorized and have keywords that can be used during a search.

To encourage use of a FRACAS database there should be a mechanism to ensure people are aware of new events that have been added.

The main reasons for operating a FRACAS is that it provides a means of managing problems and ensuring their resolution and timely closure. It also provides a means of retaining information and thus enables a company to continuously improve its products, especially in terms of reliability and quality.

12.3 Data recording and corrective action system

A DRACAS is an extended version of a FRACAS where a wider range of data than just failure data are recorded.

12.4 Lessons learned

Leading aerospace companies have identified lessons learned as a vital process to improve the competitiveness of the industry by increasing its ability to supply reliable equipment.

The key steps of a lessons learned database are:

- to identify the problem;
- to identify its root cause;
- to learn the lesson from the problem and the process of finding the root cause;
- to identify where else the lesson is applicable;
- to apply the lesson learned to the original problem and everywhere else where the lesson learned is applicable.

Implementation is best done via a database and the criteria for success include lessons learned that are:

- readily available to everyone and as self-explanatory as possible;
- categorized and have keywords that can be used during a search;
- have an alert mechanism to make people aware of new lessons;
- include lessons learned when something was successful as well as those that are solutions for problems.

Annex A – Alternative definitions and related terminology

A.1 Alternative definitions

It should be recognized that different industries use a variety of terminology for what are essentially the same concepts. The following is a listing of typical terminology.

A.1.1 Reliability

- Reliability – the ability of an item to perform its function under stated conditions for a specified period of time, i.e. it is working and does what it is supposed to do.
- Fault – the state of an item characterized by inability to perform a required function, i.e. it is not doing what it is supposed to do.
- Failure – the termination of the ability of an item to perform its function, i.e. it is broken and cannot do what it is supposed to do.
- Defect – any non-conformance of an item with specified requirements, i.e. it shows signs of being broken but may still be doing what it is supposed to do.

A.1.2 Availability

- Availability – how much of the time something is working. i.e. the uptime (when equipment is working) divided by the uptime and downtime (when the equipment is not working).

A.1.3 Maintainability

- Preventive maintenance – the routine activities to prevent failure, i.e. the servicing. This is typically done to a time or usage schedule
- Corrective maintenance – the activities required to respond to failure, i.e. the repairs.
- Predictive maintenance – the activities required to respond to an indicator of future failure, i.e. maintenance triggered by some measurement of condition.

A.1.4 Types of failure

- Damage – where the equipment has been damaged by an external event, i.e. where the damage is caused by an event outside the specification of the equipment, for example, fire, impact or operating the equipment outside its specification.
- Unplanned failure – where the equipment has failed in normal operation and it was not planned to fail, i.e. where the equipment should have worked but did not or should have been replaced before wear-out, but was not.

- Planned failure – where the equipment has failed in normal operation and it was planned to fail, i.e. where the equipment was deliberately operated up to the point of failure and the failure occurred on or after the planned for date.
- Repeat failure – where an unplanned failure has occurred and an identical (or very similar failure) has occurred before, i.e. a failure where the root cause has not been found or the lesson learned has not been implemented.

A.1.5 Causes of failure

- Early life failures – where the equipment failed unexpectedly early, i.e. failures that are likely to have been caused by poor quality of manufacture or installation.
- Through life failures – where equipment failed before reaching its expected design life, i.e. failures that are likely to have been caused by poor design, inappropriate operation or poor preventive maintenance.
- Wear out failure – where equipment has worn out, i.e. failures that are likely to have been caused by equipment being operated longer than its specified life.

A.1.6 Prevention of failure

- Root cause analysis – a process by which the underlying cause or causes of failure are identified, i.e. failure is the 'what happened?', root cause analysis is the 'why?'
- Lessons learned – a process where the root cause of a failure is identified, the actions to prevent reoccurrence defined, the items of equipment that require the action identified and a programme of work to implement the actions followed, i.e. learning the lesson and doing something about it.

A.1.7 Recording of failure

- FRACAS – A failure reporting, analysis and corrective action system, i.e. a system to log what failures have occurred, analyse why they have happened and define what needs to be done.
- DRACAS – A data reporting, analysis and corrective action system, i.e. a wider system than a FRACAS as it includes defects that have not yet caused failure.

A.2 Related terminology

A.2.1 General

The IEC 60050 definitions of reliability, maintainability and availability may not wholly apply. This is due to the converter possibly having built-in redundancy (it may be generating at partial output and, in this state, it is neither fully 'up' nor fully 'down') or

because the impact of the fault may depend on the weather, state of tide, etc, (if the converter is 'down', but there is no wave or tidal resource then there is no loss of energy generation – conversely if it is down at a period of high resource, then there is a larger loss of energy generation).

Ways of addressing this include the use of intrinsic and operational availability and the use of energy weighted availability.

A.2.2 Intrinsic and operational availability

The UK military overcome the issue of non-continuously running equipment by defining an Intrinsic Availability and an Operational Availability in the defence standard *Def. Stan 00-40 Reliability and Maintainability* as follows:

A_i	Intrinsic Availability	The probability that the system/equipment is operating satisfactorily at any point in time where the time considered is operating time and repair time. For continuously operating equipment it is: $\frac{MTBF}{MTBF + MART}$ **NOTE** This can be thought of as the best availability that can be achieved without change to increase equipment reliability or change to reduce maintenance time.
MART	Mean Active Repair Time	The time it takes to repair the system (either by component repair or replacement) excluding all other times (e.g. free time, preventive maintenance, storage time, administrative and logistic delays).
A_o	Operational Availability	The probability that an equipment/system at any instant in the required operating time will operate satisfactorily under stated conditions where the time considered includes operating time, corrective and preventive maintenance time, administrative delay time and logistic delay time. For the steady state case it is: $\frac{OT + ST}{OT + ST + TCM + TPM + ALDT}$
OT	Operating Time	The time during which the system or equipment is turned on and actively performing at least one of its functions.
ST	Standby Time	Time when the equipment is in standby mode.

TCM	Total Corrective Maintenance time	That part of the maintenance time (including that due to logistic delays) during which corrective maintenance is performed on an item. **NOTE** Including logistic delays seems to be double counting with ALDT. An interpretation is that ALDT is the time prior to starting the maintenance while the TCM included the logistic delays during the corrective maintenance.
TPM	Total Preventive Maintenance time	The maintenance carried out at predetermined intervals or according to prescribed criteria intended to reduce the probability of failure or the degradation of the functioning of an item. **NOTE** In this context preventive maintenance time includes predictive maintenance time.
ALDT	Administrative and Logistic Delay time	The accumulated time during which an action of corrective maintenance on a faulty item is not performed due to administrative reasons. (IEC-60050(191)) Logistic delay is the time which a maintenance activity cannot be performed due to the necessity to acquire maintenance resources. (IEC-60050(191))

In the context of a marine energy converter, the standby time would include grid outages, grid operating company instructed outages, time when there is no resource and time when there is no demand.

A.2.3 Energy weighted availability

The IEC definition does not adequately reflect the conditions for renewable energy where the equipment's ability to run at rated capacity fluctuates with the availability of the resource.

An alternative measure of availability is based on the energy generated terms by a three-stage process involving:

- Rated capacity – which reflects the inherent capability of the machine;
- Capacity factor – which reflects the matching of the machine to the resource;
- Energy weighted availability – which reflects the reliability and maintainability of the machine.

The energy weighted availability equates to:

$$\frac{\text{energy generated}}{\text{energy generated} + \text{lost energy generation during downtime}}$$

The average power developed by a generator is the rated capacity × capacity factor × energy weighted availability.

Assessing the energy weighted availability is dependent on the ability to know, either by calculation or measurement, the resource available. This measure is therefore more appropriate to tidal stream devices where the streams can be readily calculated and measured.

Annex B – Improvement through change

B.1 Reliability improvement

Reliability, maintainability and survivability will only improve by application of this guide if it is used to deliver change. There are many ways to improve reliability and availability. Typical options for change that are available include:

B.1.1 Design improvement

- Integrity:
  - improve operating margins by improving equipment design;
  - reduce the occurrence of failure by improving equipment design.
- Resilience:
  - improve the resilience to failure by adding equipment redundancy;
  - improve the resilience by adding systems that allow reconfiguration so operations can continue with faults, failures or defects.

B.1.2 Maintenance improvement

- Preventive maintenance:
  - replace old with new;
  - identify degradation prior to failure;
  - repair/replace before failure;
  - extend the time to failure;
  - minimize the repair time.
- Corrective maintenance:
  - minimize the repair time;
  - minimize repeat failures;
  - ensure root cause (rather than symptom) is identified and repaired.
- Predictive maintenance:
  - target maintenance by measuring the correct indicators of incipient failure.

B.1.3 Operations

- Engineering operations:
  - improve spares availability;
  - improve tools availability;
  - improve staff availability, reaction times and get to site times.
- Service operations:
  - operate system to minimize unnecessary stress on equipment;
  - contingency measures to provide temporary work around solutions to failure.

B.2 Availability improvement

For deployed systems improvement in corrective maintenance time following a fault is often the route to the improvement in availability as the scope for design or operational change may be limited. Typical activities where there are options for change are:

- identification time – what has gone wrong;
- localization time – where it has gone wrong;
- isolation time – isolating the fault so that it can be repaired;
- mobilization time – mobilizing the people, spares and tools to the scene;
- repair time – repairing the equipment;
- recovery time – removing the people and setting the system to work again;
- approval time – gaining any approvals required to restart.

Annex C – Improvement through testing

C.1 General

The importance of a structured programme of system and component testing prior to installation towards reliability cannot be overemphasized.

It is also important to distinguish between performance testing and reliability testing.

C.2 Types of testing

This testing falls into two categories – development testing and production testing.

C.3 Purpose of testing

The purpose of development testing is mainly to confirm the strengths in the design and identify any weaknesses in the design.

The purpose of production testing is mainly to identify any manufacturing weaknesses.

Production testing should not be used to identify weaknesses in the design.

C.4 Depth of testing

Testing, and in particular design for testability, should be an integral part of the design, development and production process. Testing options include:

- laboratory testing;
- environmental testing;
- water tank testing (fresh water);
- water tank testing – indoors (sea water);
- water tank testing – outdoors (sea water);
- at sea testing – sheltered site;
- at sea testing – test site;
- at sea testing – installation site.

Annex D – Improvement through managing offshore operations

D.1 General

The importance of understanding what offshore operations will be required, the resources required for them and the sea conditions that exist to allow them to happen cannot be over emphasized.

D.2 Types of operations

These operations include:

- installation operations;
- servicing operations;
- maintenance operations;
- repair and replacement operations;
- removal operations.

D.3 Reversibility of operations

It is also important to note that each operation has to be reversible. In other words if the intended operation goes wrong and cannot be completed, it must be possible to reverse it to the point where the device is in a survivable (and preferably operational) state and the resources withdrawn.

D.4 Availability of vessels

The type and availability of vessel required for installation, operations and maintenance should also be an integral part of the design. Specialist vessels, such as jack-ups, crane barges and tugs, have restricted availability and high cost. A design that can use a wide range of vessels and is not tied to a particular vessel is likely to have higher availability.

D.5 Time taken for operations

The time taken for operations is critical. For most operations there will be a finite period of time available based on:

- daylight;
- wave conditions;

- tide conditions;
- wind conditions;
- weather conditions (rain, fog, snow, lightning, temperature, etc);
- duration of permits;
- safe systems of work constraints;
- isolation time.

D.6 Safety of operations

Offshore operations, particularly those that involve people accessing structures and devices from boats, are hazardous, so consideration of access should be an integral part of the design, installation and maintenance concept.

For more information on safety, please see *Guidelines for Health and Safety in the Marine Energy Industry* in the Marine Renewable Energy Guides series.

Annex E – Example of analysis worksheets

E.1 FMECA

Item	Failure Mode	Probability	Failure Effect- Local	Failure Effect - End	Detection	Compensating Provisions	Consequence	Risk	Remarks

Figure E.1 — FMECA worksheet

E.2 HAZOP

Item or Function	Guide Word	Deviation	Possible Causes	Consequences	Cons.	Prob.	RPN	Risk Rank	Action Required

Figure E.2 — HAZOP worksheet

E.3 Maintenance task analysis

Ref.	Maintenance Task	Type	Resources Required	Parts Required	Consumables Required	Environmental Conditions Required	Task Duration	"On" During Maintenance	Related Failure Modes
		Preventive							
		Corrective							

Figure E.3 — Maintenance task analysis worksheet

E.4 Lessons learned

Ref.	Problem	Source	Root Cause(s)	Lessons Learnt	Applicability	Design Features to Incorporate Lesson	Operation Features to Incorporate Lesson	Action

Figure E.4 — Lessons learned log

Annex F – Example of risk assessment methods

F.1 General

There are many methods for assessing levels of risk. The following sections outline two possible methods:

- a technology assessment method – this is recommended by the Carbon Trust for wave energy converters and is a judgement of technical novelty based on the technology and its application;
- a technology readiness level method – this is used by oil and gas companies for subsea projects and is a judgement of the technical risk plus the ability of organizations to manage the technical risk.

F.2 Technology assessment method

The method favoured by the Carbon Trust in their publication, *Guidelines on design and operation of wave energy converters* (which in turn is based on DNV RP-A203) is based on the formula:

- Technical novelty = Application area × Technology maturity

The application area is chosen from either Known Application or New Application and the technology maturity is chosen from Proven Technology, Limited field history or New or unproven.

The technical novelty is then assigned using a matrix:

Application Area	Technology		
	Proven	Limited field history	New or Unproven
Known	1	2	3
New	2	3	4

1 No new technical uncertainties
2 New technical uncertainties
3 New technical challenges
4 Demanding new technical challenges

Figure F.1 — Technology assessment matrix

The strength of this method is that it is quick and easy.

The weakness is that for new technologies where there is uncertainty the technical novelty in itself is not a measure of risk. Technical novelty may reduce risk as well as increase it.

F.3 Technology readiness level method

A method used by the subsea oil and gas industry builds on the technology assessment method of DNV. In effect, it is based on the observation that high reliability is a function of both the technology and the capability of the organizations involved to design, build, operate and maintain it, which is based on:

Technical readiness = Technical readiness of the equipment × Technical readiness of the organizations

This is sometimes described as:

Risk = Equipment maturity × Organizational capability

Proven technology designed and operated by capable organizations will be the lowest risk whilst unproven technology designed and operated by an uncontrolled organization will be the highest risk.

Examples of matrices used to apply this approach are given in Figures F.2 and F.3, however, suitable matrices should be selected by the organizations applying the method.

The equipment maturity is chosen from the following:

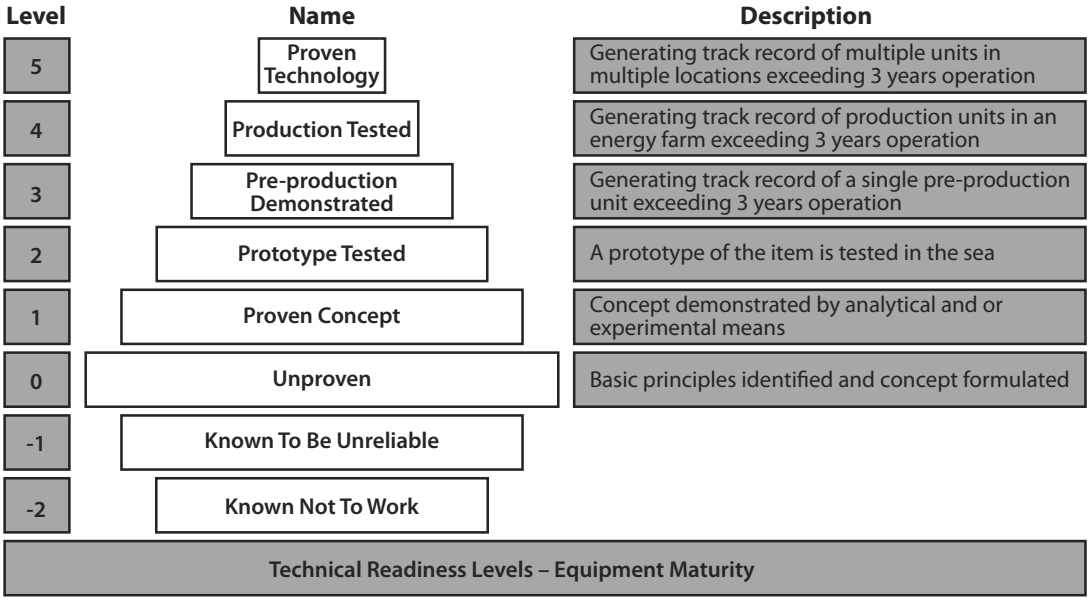

Figure F.2 — Equipment maturity

The organizational capability is chosen from the following:

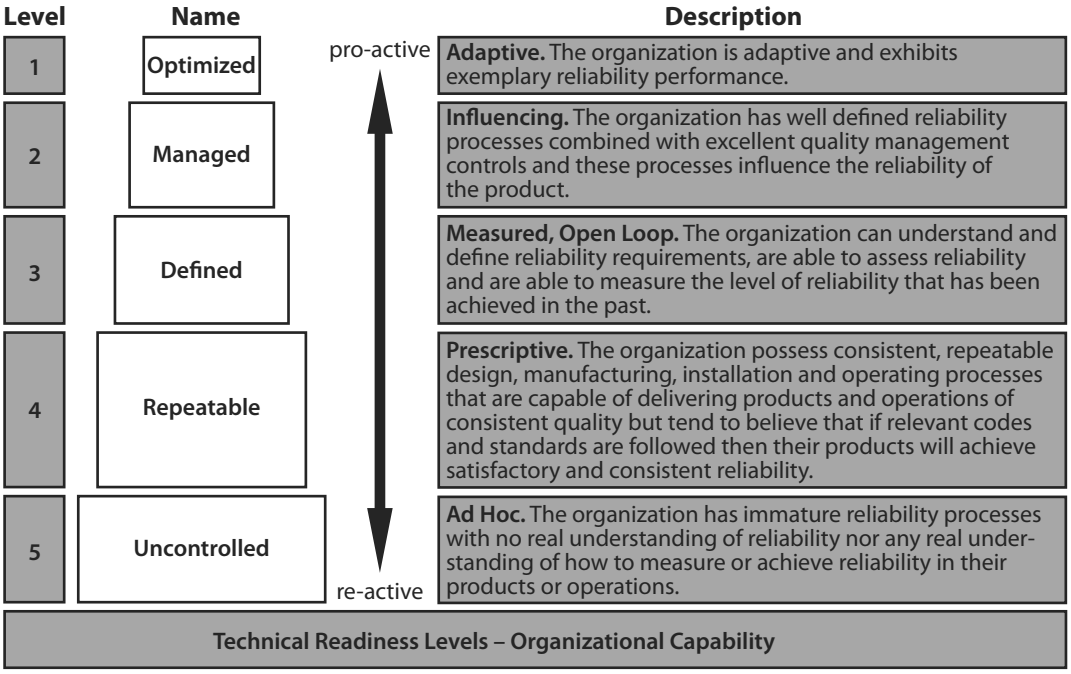

Figure F.3 — Organizational capability

The technical readiness is then assigned using a matrix:

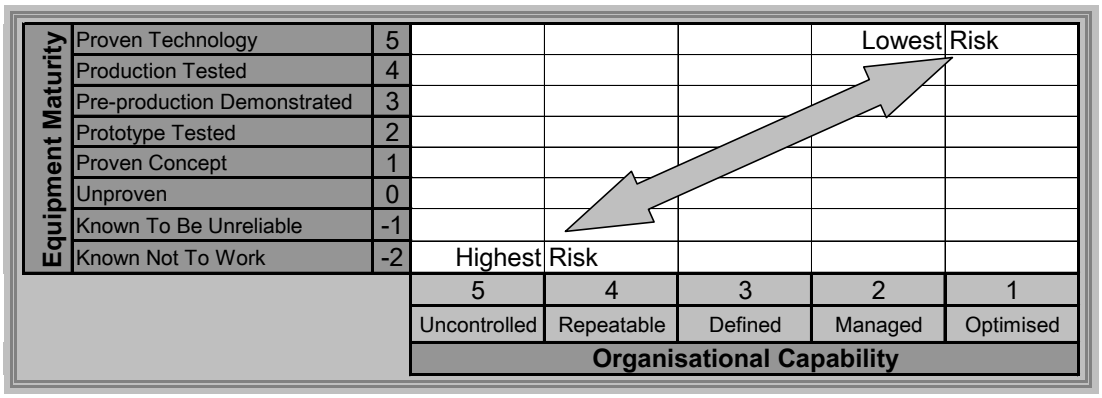

Figure F.4 — Technical readiness matrix

Bibliography

DNV RP-A203 *Qualification procedure for new technology*

API RP 17N *Recommended practice for subsea production system reliability and technical risk management*

ISO 20815:2008, *Petroleum, petrochemical and natural gas industries: Production assurance and reliability management*