

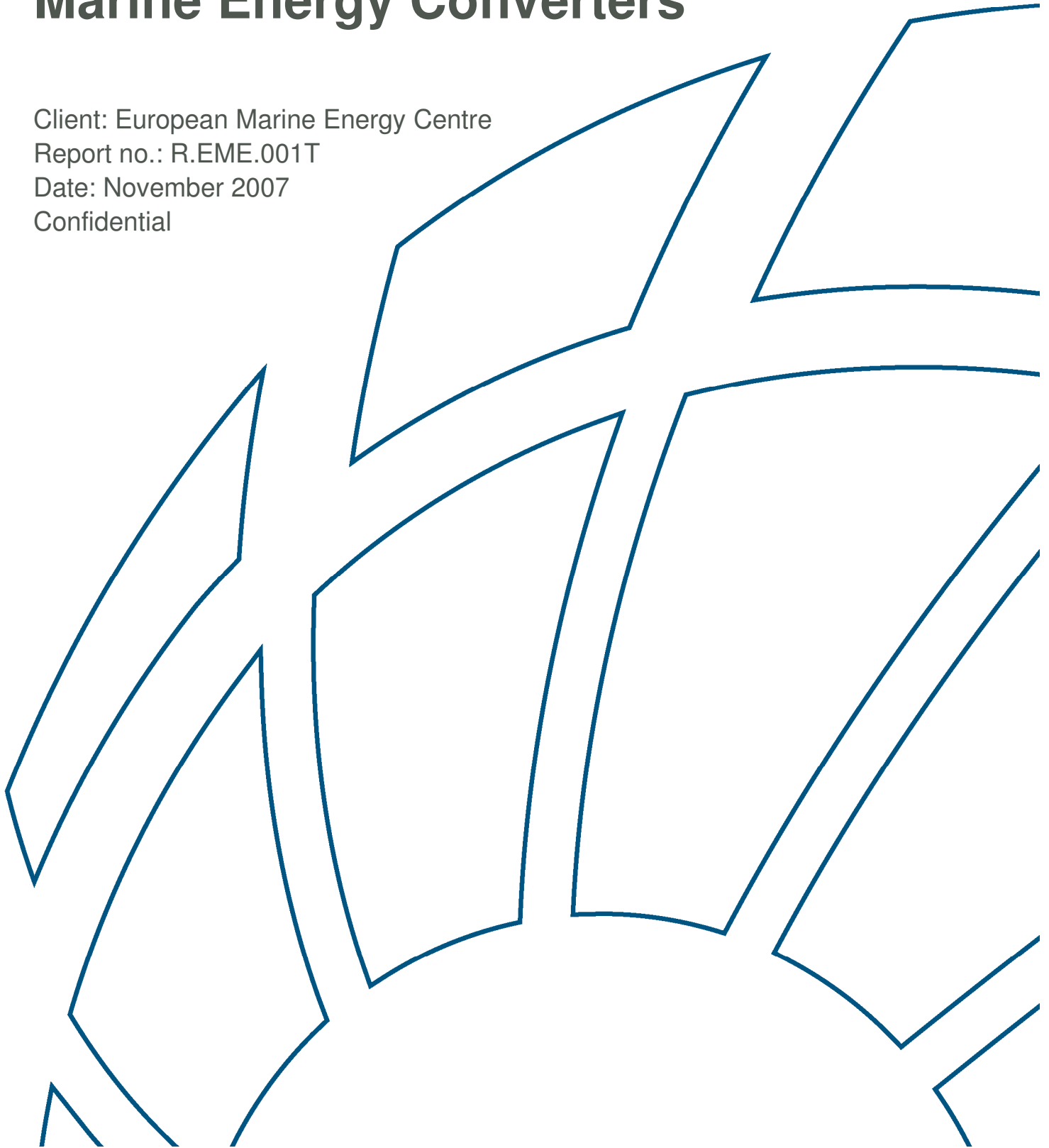
Draft Standard on Reliability, Maintainability and Survivability for Marine Energy Converters

Client: European Marine Energy Centre

Report no.: R.EME.001T

Date: November 2007

Confidential



Intentionally blank page

draft for consultation

Report Title	Draft Standard on Reliability, Maintainability and Survivability for Marine Energy Converters
Client	European Marine Energy Centre
BMT Cordah Report No:	R.EME.001T
Status and Version:	Working Draft
Date of Release:	November 2007
Terms:	The contents of this report are confidential. No part thereof is to be cited without the express permission of BMT Cordah Ltd or the European Marine Energy Centre.

	Name	Signature	Position	Date
Author	Michael Starling			
Reviewed by	{Checker}			
Approved by	{Approver}			

BMT Cordah Limited,

4th Floor,
Holland House,
1 – 4 Bury Street,
London
EC3A 5AW

Tel. +44 (0)20 7015 0300

Fax +44 (0)20 7015 0344

Email: enquires@bmtcordah.com

Website: www.bmtcordah.com

Document log

Version	Date	Summary of changes	Author
Working Draft	27 November 2007	Initial draft for circulation within EMEC, BMT and the Technical Committee	Michael Starling

draft for consultation

CONTENTS

Forward	6	
Introduction	8	
1	Scope	9
2	Normative references	9
3	Terms and definitions	10
3.1	Reliability	10
3.2	Maintainability	10
3.3	Survivability	10
3.4	Availability	11
3.5	Units	12
4	Importance of reliability, maintainability and survivability	13
5	Reducing Reliability Risk	14
5.1	Risk Assessment - Technology Assessment Method	14
5.2	Risk Assessment - Technology Readiness Level Method	15
5.3	Scalability of the Risk Assessment Methods	17
5.4	Important note	17
6	Defining reliability, maintainability and survivability targets	18
6.1	Energy Farm Requirements	18
6.2	Device Requirements	18
6.3	Device Requirement Specification	21
7	Design for reliability, maintainability and survivability	23
7.1	Mature Industry Approaches	23
7.2	Early Industry Processes	24
8	Assurance requirements for reliability-maintainability-survivability	25
8.1	Typical Reliability Assurance Process	25
8.2	Concept of the Reliability Case	25
9	Potential Tools	30
9.1	Failure Modes Effects and Criticality Analysis (FMECA)	30
9.2	Hazard and Operability Studies (HAZOP)	30
9.3	Maintenance Task Analysis	31
10	Improving reliability from prototype and operational feedback	32
10.1	Failure Reporting And Corrective Action System (FRACAS)	32
10.2	Data Recording and Corrective Action System (DRACAS)	32

10.3	Lessons Learned Databases	33
Bibliography		34
Annexes		
11	Annex A - Other Commonly Used Definitions	35
11.1	Reliability	35
11.2	Availability	35
11.3	Maintainability	35
11.4	Types of Failure	35
11.5	Causes of Failure	36
11.6	Prevention of Failure	36
11.7	Recording of Failure	36
12	Annex B - Improvement through Change	37
12.1	Reliability Improvement	37
12.2	Availability Improvement	38
Figures		
Figure 1	Technology Assessment Risk Matrix	15
Figure 2	Equipment Maturity	16
Figure 3	Organisational Capability	16
Figure 4	Technical Readiness Risk Matrix	17
Figure 5	Maximum Probability of Premature Failure - Example Calculation	22
Figure 6	Reliability Key Processes - Project Processes	23
Figure 7	Reliability Key Processes - Common Processes	23
Figure 8	Typical Iterative Reliability Assurance Process	25
Figure 9	Example Evidence Quality Categorisation	27
Figure 10	Example FMECA Worksheet	30
Figure 11	Example HAZOP Worksheet	31

Figure 12 Example Maintenance Task Analysis Worksheet	31
Figure 13 Example Lessons Learned Log	33

draft for consultation

Forward

Publishing information

This is a working draft of an unpublished standard/guide. It has been written in the style of a British Standards Institution (BSI) standard for ease of future adoption.

Supersession

The document is new.

Relationship with other publications

This document is part of a suite of standards/guides covering the validation and verification of marine renewable devices in the areas of:

- device development
- scheme development
- assurance

Device development standards/guides include:

- manufacture & testing
- tidal tank test and wave tank test
- tidal performance testing and wave performance testing

Scheme development standards/guides include:

- project development
- tidal resource assessment and wave resource assessment
- grid interface

Assurance standards/guides include:

- health & safety
- design basis (including install, mooring and foundations)

- reliability, maintainability and survivability (this document)
- environmental impact

Information about this document

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 including:

- Marine Energy Standards Workshop
 - sponsored by E.ON and held at the National Motorcycle Museum, West Midlands, on the 7th March 2007
- Marine Energy Standards Workshop
 - sponsored by Scottish and Southern Energy and held at Institution of Electrical Engineers, Glasgow, on the 26th September 2007

It has been produced under the guidance of:

- Ad Hoc Working Group on Marine Energy Standards (superseded by)
- Technical Committee PEL/114 - Marine Energy - Wave and Tidal Energy Converters

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Introduction

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

It recognises that the industry is in its infancy and that the standard/guide should be capable of flexible and beneficial application to:

- concept designs
- prototypes under development
- pre-production installations
- experimental marine energy farms.

Typical application may include:

- All Stages
 - to make sure that at all stages of development the requirements for reliability-maintainability-survivability for a deployed energy farm are identified and are deconstructed into device level requirements
- Concept Stage
 - to make sure that there are not any long term reliability-maintainability-survivability risks that cannot be resolved during the project development
- Prototype Stage
 - to avoid critical failures that can put off investors or give the product/process a bad name
- Pre-production Stage
 - to design in reliability-maintainability-survivability at the pre-production stage
- Energy Farm Stage
 - to build device level reliability-maintainability-survivability performance (and predictions) into an estimate of performance of the deployed energy farm

1 Scope

It is intended that this standard/guide can be used to improve and/or demonstrate the reliability-maintainability-survivability of marine energy devices that:

- extract energy from waves
- extract energy from tides and tidal streams

The standard/guide is goal based, in that it takes as its starting point definition of the reliability-maintainability-survivability requirements for a successful and economic energy farm and flows these requirements down to the individual device and the tools and techniques to help meet these requirements.

The standard/guide is flexible, in that it does not define a set way of doing things but defines a range of techniques that can be used.

2 Normative references

The following referenced documents are 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.*

3 Terms and definitions

3.1 Reliability

The IEC 600050 definition is:

- The probability that an item can perform a required function under given conditions for a given time interval. (IEC 600050 - 191-12-01)

3.2 Maintainability

The IEC 600050 definition is:

- The 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 600050 - 191 - 13 - 01)

3.3 Survivability

No definition of survivability has been found in international standards.

The current definition in Wikipedia is:

- In engineering, **survivability** is the quantified ability of a system, subsystem, equipment, process, or procedure to continue to function during and after a natural or man-made disturbance.

However this does not adequately cover both aspects of survivability in the marine environment so the following definitions are proposed:

- the ability to survive discrete events
 - such as major storms, peak waves etc.
- the ability to survive the cumulative effects of the marine environment over time
 - such as the cumulative battering of the waves or the long term corrosion effects

3.4 Availability

The IEC 600050 definition is:

- 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. (IEC 600050 - 191 - 02 - 05)

For continuously running equipment this equates to:

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

3.4.1 Energy Weighted Availability

However this 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.

Availability therefore has to be measured in 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 x Capacity Factor x Energy Weighted Availability

3.5 Units

There is confusion in the public mind between energy and power. Care should be taken when preparing technical documents that may appear in the public domain to clearly differentiate between them.

3.5.1 Energy Generated

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.

3.5.2 Power Generated

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

4 Importance of reliability, maintainability and survivability

Reliability, maintainability and survivability are crucial to the economic case for a marine energy generator. Their effect:

- Capital Expenditure (CapEx)
- Revenue (RevEx)
- Operational Expenditure (OpEx)
- Risk Expenditure (RiskEx)

In particular:

- the design of the equipment (CapEx)
- the energy generated by the machines and hence the revenue to the project (RevEx)
- the cost of maintenance of the machines and hence the operational costs of the project (OpEx)
- the risks to the project (RiskEx) including:
 - ability to raise investment and the cost of the investment
 - ability to insure and certify and the cost of insurance
 - effect on the asset/safety/environment of failure and the cost to rectify

5 Reducing Reliability Risk

Reliability-maintainability-survivability are a feature of a design that are competing for resources. One of the methods for deciding the relative priorities for resource is to assess the level of risk.

There are many methods for doing this. The following sections outline two possible methods:

- a Technology Assessment method
 - recommended by the carbon trust for wave energy converters
- a Technology Readiness Level method
 - as used by Oil & Gas companies for subsea projects

5.1 Risk Assessment - Technology Assessment Method

The method favoured by the Carbon Trust in their Guidelines on design and operation of wave energy converters - a guide to assessment and application of engineering standards and recommended practices for wave energy conversion devices (which in turn is based on DNV RP-A203) is based on:

- Risk = Application Area x Technology Maturity

5.1.1 Step 1 - Application area

The application area is chosen from:

- Known
- New

5.1.2 Step 2 - Technology maturity

Technology maturity is chosen from:

- Proven
- Limited field history
- New or unproven

5.1.3 Step 3 - Risk

The risk level is then assigned using a risk 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 1 Technology Assessment Risk Matrix

5.2 Risk Assessment - Technology Readiness Level Method

A method used by the subsea Oil & 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 organisations involved to design, build, operate and maintain it:

It is based on:

- Risk = Technical Readiness of the Equipment x Technical Readiness of the Organisations

This is sometimes described as:

- Risk = Equipment Maturity x Organisational Capability

Proven technology designed and operated by capable organisations will be the lowest risk while unproven technology designed and operated by an uncontrolled organisation will be the highest risk.

An example of matrices used to apply this approach are given below. However suitable matrices should be selected by the organisations applying it.

5.2.1 Step 1 - Equipment Maturity

The equipment maturity is chosen from the following:

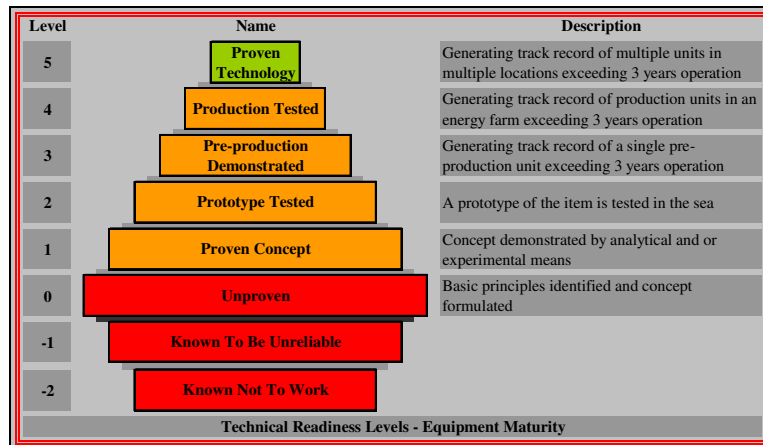


Figure 2 Equipment Maturity

5.2.2 Step 2 - Organisational Capability

The organisational capability is chosen from the following:

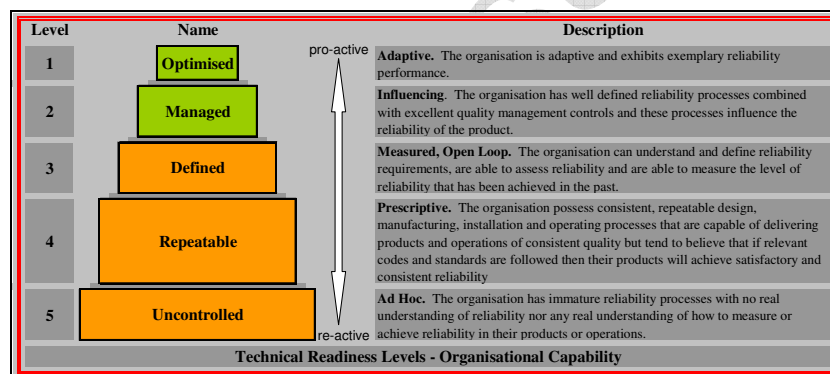


Figure 3 Organisational Capability

5.2.3 Step 3 - Risk

The risk level is then assigned using a risk matrix:

Equipment Maturity	Proven Technology	5						Lowest Risk
	Production Tested	4						
	Pre-production Demonstrated	3						
	Prototype Tested	2						
	Proven Concept	1						
	Unproven	0						
	Known To Be Unreliable	-1						
	Known Not To Work	-2	Highest Risk					
		5	4	3	2	1		
		Uncontrolled	Repeatable	Defined	Managed	Optimised		
		Organisational Capability						

Figure 4 Technical Readiness Risk Matrix

5.3 Scalability of the Risk Assessment Methods

These approaches are scalable in that they can be applied:

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

5.4 Important note

It is important to note that a low level of reliability risk does not necessarily equate to a high level of reliability and vice versa. The level of risk equates to the level of uncertainty that can be attached to any prediction of reliability performance.

6 Defining reliability, maintainability and survivability targets

6.1 Energy Farm Requirements

Marine energy converters are generally anticipated to be used in farms with multiple generators. The reliability, maintainability and survivability requirements for the device flow from the fundamental business case for the farms. This is likely to result in two key parameters:

- the required energy weighted availability
- the maximum operating cost for achieving the availability

6.2 Device Requirements

To flow the energy weighted availability requirement down into a technical requirement for a device it is necessary to understand the factors that are included in it.

6.2.1 Factors Affecting Device Requirements

These include:

- configuration
 - number of devices
 - location of devices
 - number of offshore sub-stations
 - offshore cable architecture (inter-array and export cables)
 - onshore cable architecture to grid connection point
- energy generation
 - power curves
- reliability
 - failure rate
 - failure effect

- repair action
- maintenance and repair actions
 - maintenance task frequency
 - maintenance task duration
 - required resources
 - required metocean conditions
- metocean data
 - forecast wind speed and direction
 - forecast wave height, period and direction
 - current speed
 - water depth
 - daylight and visibility
 - sea ice
 - “run for cover” storms
- other environmental data
 - temperature
 - rain
 - lightning
- resources
 - types and numbers of vessels
 - their location
 - their capability

6.2.2 Combining Generic and Site Specific Factors

The effects of these factors are a combination of those generic to the machines (e.g. for energy generation) and other 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. For example is it more likely to fail (or more difficult to fix) during periods of good energy resource?

6.2.3 Requirements for Metocean Data

Length of Data Record

The data record used should cover as long a time as reasonably possible. This should be ideally over 10 years to get statistical significance for regular operation phenomena.

Note that even 10 years will not be adequate for assessing the risk of extreme events: such events should be considered along with the “return period” criteria typically used in, for example, foundation design.

Near Shore Effects

Note that many sites considered for wind, tidal and wave energy are quite near-shore, in areas of shallow water. Consideration shall be given to the appropriateness of any metocean data for such sites: much metocean data is 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 is used to represent the site in question.

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

Need for Correlated Data

It is important that the metocean data is either:

1. in the form of a correlated time history
2. or if this is not available the it should be in the form of a probability distribution of weather windows for the required combinations of wind speed, wave height, current and duration.

For example, within the next D days, what is the probability of:

- a period of T hours with

- wind speed < W m/s AND
- significant wave height < H m AND
- current (absolute) < C m/s AND
- good visibility

However it should be noted that option 2 is a *multi-dimensioned* probability distribution. This means that it can only be generated from a correlated time series, i.e. option 1.

6.3 Device Requirement Specification

6.3.1 Traditional Methods for Specifying Device Reliability

The traditional method for specifying device reliability is by:

- Mean Time Between Failures (MTBF)
- Mean Time to Repair (MTTR)

However in the context of marine energy devices it is unlikely that these measures can be derived from energy farm requirements or known device achievement extrapolated into expected energy farm performance.

6.3.2 Appropriate Methods for Specifying Device Reliability

Where the ability to maintain a device is constrained by time (for example a summer maintenance season or to coincide with the availability of a boat) a better way of specifying device 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
 - 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

The following is an example of a calculation of the maximum probability of premature failure.

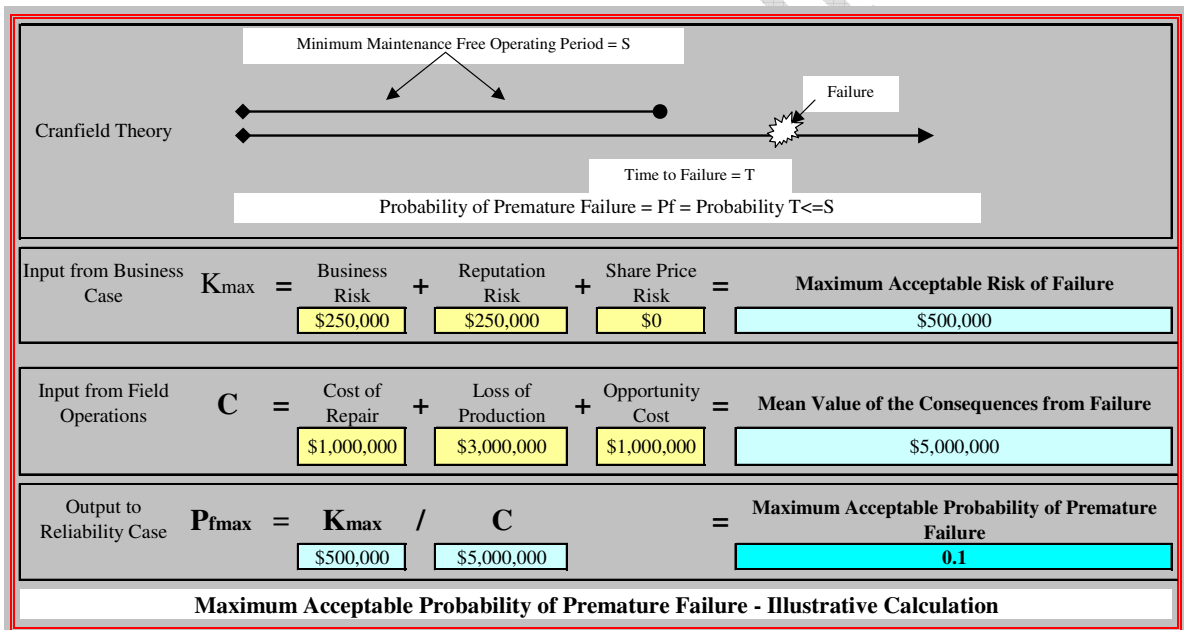


Figure 5 Maximum Probability of Premature Failure - Example Calculation

7 Design for reliability, maintainability and survivability

7.1 Mature Industry Approaches

The American Petroleum Institute have identified 14 key processes for reliability and technical risk management for subsea production systems. These are divided into two groups:

- processes that occur at defined stages of a project
- common processes that occur at all stages of a project

These are summarised below:

R&M Key Processes	Project Stage						
	Feasibility	Concept Selection	FEED	Detailed Design	Manufacture	SIT/Installation/ Commissioning	Operations
1. Definition of R&M Goals and Requirements	X	X	X	X	X	X	X
2. Organizing and Planning for R&M	X	X	X	X	X	X	X
3. Design and Manufacture for R&M			X ¹	X ¹	X		
4. Reliability Assurance	X	X	X	X	X	X	X
5. Risk and R&M Analysis		X	X	X	X	X	X
6. R&M Qualification and Testing	X ¹	X ¹	X ¹	X ¹	X ¹	X ¹	X ¹

Figure 6 Reliability Key Processes - Project Processes

7. Verification and Validation
8. Project Risk Management
9. Performance Tracking and Data Management
10. Supply Chain Management
11. Management of Change
12. Organizational Learning

Figure 7 Reliability Key Processes - Common Processes

7.2 Early Industry Processes

The marine energy converter business is not mature and applying mature industry process to it is unlikely to be financially possible. However it is possible to recommend some key processes that should be followed.

- Requirements Definition
 - defining and managing reliability targets during the design stage
- Reliability Improvement
 - data collection, reliability analysis and improvement during design
- Performance Monitoring
 - collecting and correlating device performance with operational circumstances
- Design for Ease of Maintenance
 - design of maintenance and recovery systems to be based on accessibility for maintenance

8 Assurance requirements for reliability-maintainability-survivability

The recommended process for reliability assurance is to:

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

8.1 Typical Reliability Assurance Process

The fundamentals of a reliability 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 the diagram below.

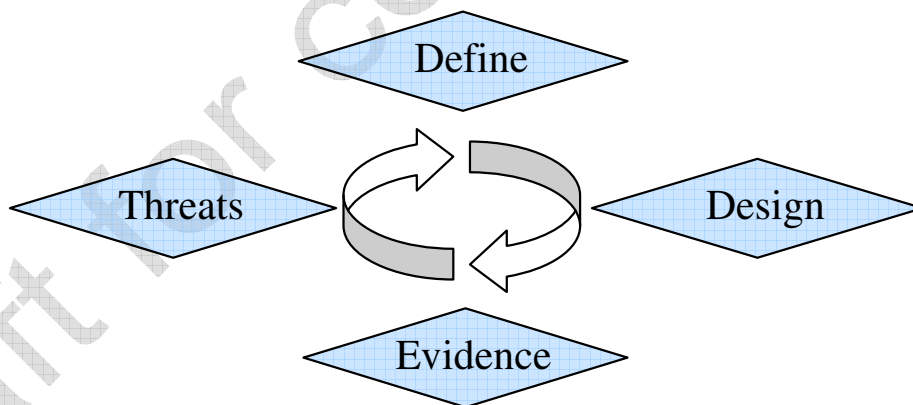


Figure 8 Typical Iterative Reliability Assurance Process

8.2 Concept of the Reliability Case

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

The Reliability Case has grown out of the economic imperative for high reliability and the operational imperative of maintenance free operating periods.

Traditional techniques alone cannot achieve these high levels of reliability as they rely on calculation, overlook evidence and rarely lead to change.

Critically traditional techniques ignore early life failures, leading to systems that fail at the worst time when introducing a new products or services.

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

8.2.1 Evidence of Success

The Reliability Case is centred around finding evidence of success. At the start of the process it is assumed that there is “no evidence that the system or process will work” and the Reliability Case aims to find evidence to “show that it will work”.

This leads to the correct inference that:

- “if you have not shown that it will work then you cannot claim that it will”

At the start of traditional reliability processes there is an implicit assumption “that the system or process will work” and the traditional techniques aim to “show how it might fail”.

This leads to the false inference that:

- “if you have not shown it will fail you have shown that it will work”.

Absence of evidence (correctly) weakens a Reliability Case, absence of evidence (incorrectly) strengthens traditional techniques.

8.2.2 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 with the current in service operation and trials examples of the best evidence and no evidence and verbal expert opinion examples of the worst evidence.

It is important to note that good evidence does not automatically lead to a good reliability case, it may be excellent evidence that shows that it will not work. **It is important that all the evidence found is used, evidence supporting reliability and evidence challenging it.** Honesty in the use of evidence is required.

An example of a formal evidence categorisation system we have used is shown below.

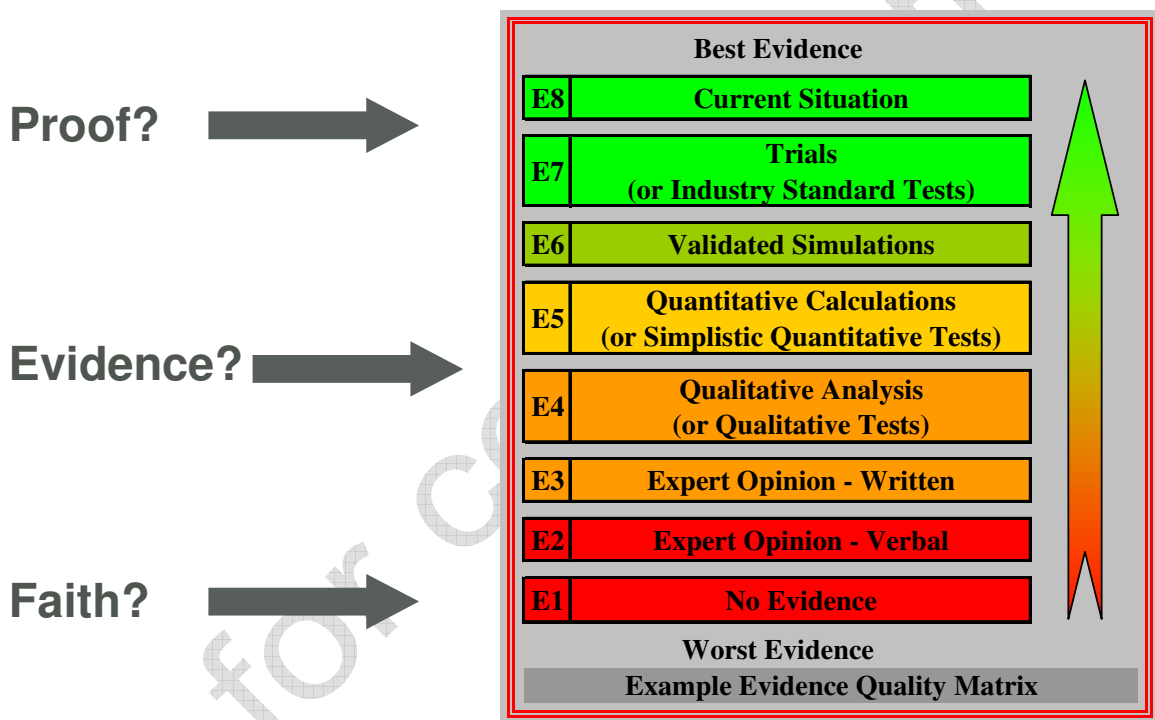


Figure 9 Example Evidence Quality Categorisation

8.2.3 Reliability Case Process

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

- o producing **reliability requirements** matched to the operational and financial requirements
- o seeking **evidence** that requirements will be met
- o 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 which is scrutinised by the management process.

8.2.4 Building Up Evidence of Success

Obtaining and scrutinising evidence is crucial to the reliability case. 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 reliability case the evidence is being used to support
- an assessment of the evidence together with a formal categorisation of its quality
- the importance of the evidence to the Reliability Case
- the actions required to obtain more evidence
- recording the build-up of evidence in an Evidence Register so it can be scrutinised

8.2.5 Building-up a Reliability Case

By focussing on evidence of success the Reliability Case approach is a significant change from existing assurance techniques. Design solutions and the evidence that supports the claim that the design solution will meet the performance required should be rigorously searched for and scrutinised. Analysis should include:

- the proposed solution and its purpose
- the evidence and quality of evidence supporting the Reliability Case
- a reasoned argument supporting the claim
- and the gaps in the evidence
- recording the build-up of the Reliability Case so it can be scrutinised

8.2.6 Assessing the Strength of a Reliability Case

The process of assessing the strength of a Reliability Case involves an assessment of the quality and relevance of the different evidence presented and the strength and completeness of the arguments used.

The advantages of this type of formalised approach is that it allows the integrity of the evidence to be examined as a whole. For example it can identify:

- evidence that is used in a large number of claims and is therefore critical to success
- the most beneficial new evidence to obtain
- 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

9 Potential Tools

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

- Failure Modes Effects and Criticality Analysis
- Hazard and Operability Studies
- Maintenance Task Analysis

9.1 Failure Modes Effects and Criticality Analysis (FMECA)

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

An example worksheet is shown below.

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

Figure 10 Example FMECA Worksheet

9.2 Hazard and Operability Studies (HAZOP)

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 to other areas as well.

It 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.

An example worksheet is shown below.

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

Figure 11 Example HAZOP Worksheet

9.3 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 and the ability of the generator to keep on generating during maintenance.

An example worksheet is shown below.

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

Figure 12 Example Maintenance Task Analysis Worksheet

10 Improving reliability from prototype and operational feedback

There are also a large number of tools that are available to manage prototype and operational feedback and this standard does not attempt to list them all. Instead its list some of the principal tools and the benefits from using them. These are:

- Failure Reporting And Corrective Action System (FRACAS)
- Data Recording and Corrective Action System (DRACAS)
- Lessons Learned

10.1 Failure Reporting And Corrective Action System (FRACAS)

A FRACAS is a closed loop activity that records and collates information in a database which 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 categorised and have key words that can be used during a search.

To encourage use of 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.

10.2 Data Recording and Corrective Action System (DRACAS)

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

Bibliography

DnV RP A-203	Qualification of New Technology
API RP 17N	Recommended Practice. Subsea Production System Reliability & Technical Risk Management

draft for consultation

11 Annex A - Other Commonly Used Definitions

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

11.1 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 characterised 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

11.2 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).

11.3 Maintainability

Preventive Maintenance – the routine activities to prevent failure.

i.e. the servicing. 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

11.4 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

11.5 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 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

11.6 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

11.7 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 defect reporting, analysis and corrective action system.

i.e. a wider system than a FRACAS as it includes defects that have not yet caused failure

12 Annex B - Improvement through Change

12.1 Reliability Improvement

Reliability-maintainability-survivability will only improve by application of this standard/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:

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

Maintenance Improvement

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

Operations

- Engineering Operations
 - improve spares availability
 - improve tools availability
 - improve staff availability, reaction times and get to site times
- Service Operations
 - operate system to minimise unnecessary stress on equipment

- contingency measures to provide temporary “work around” solutions to failure

12.2 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
- Localisation Time
 - where it has gone wrong
- Isolation Time
 - isolating the fault so that it can be repaired
- Mobilisation Time
 - mobilising 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