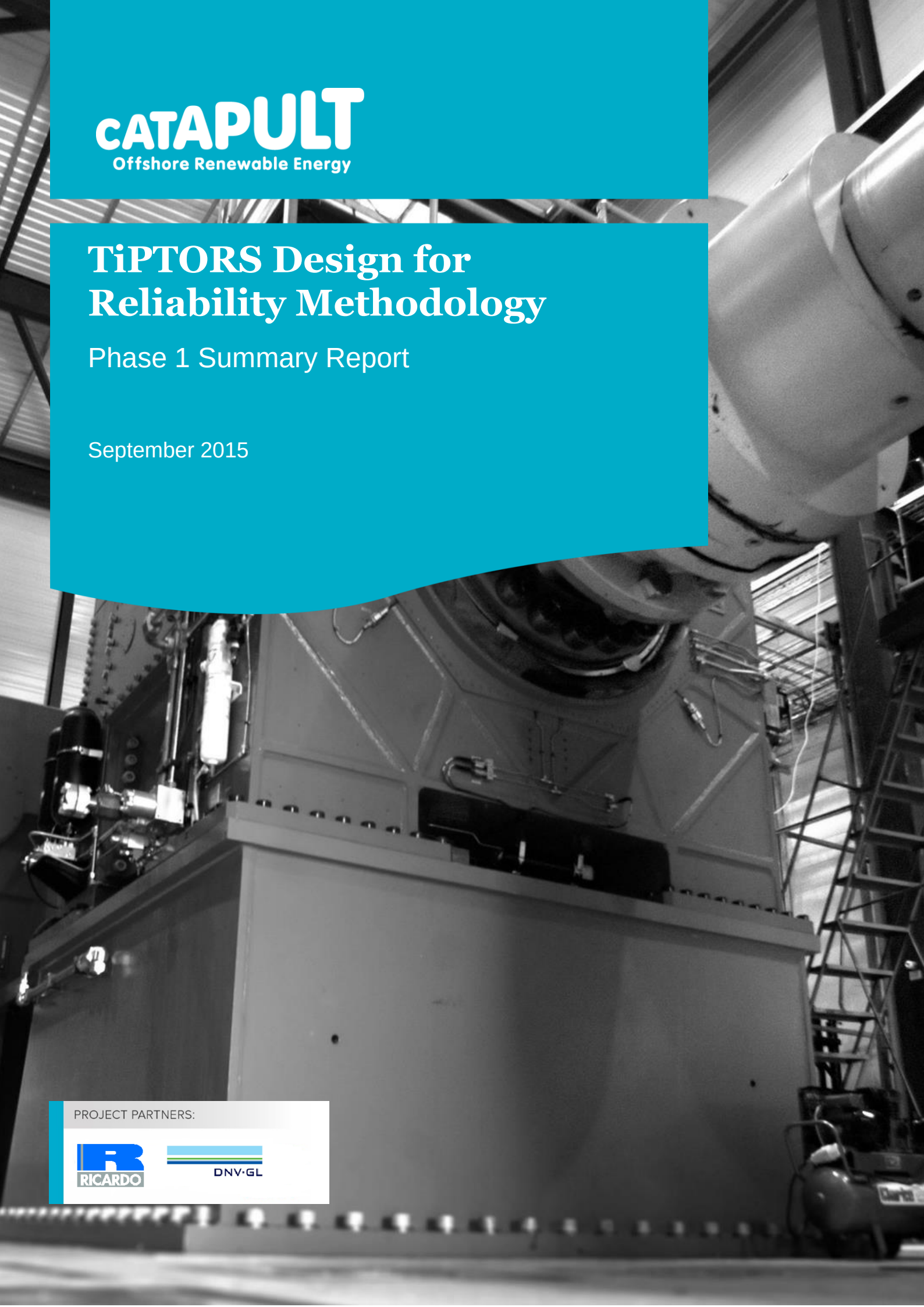

CATAPULT
Offshore Renewable Energy

TiPTORS Design for Reliability Methodology

Phase 1 Summary Report

September 2015

PROJECT PARTNERS:

RICARDO

DNV·GL

Document History

Field	Detail
Report Title	TiPTORS Design for Reliability Methodology
Report Sub-Title	Phase 1 Summary Report
Client/Funding	Collaboration
Status	Public
Project Reference	PN000047
Document Reference	PN000047-SRT-001

Revision	Date	Prepared by	Checked by	Approved by	Revision History
1.0	Aug 2015	R Browett	P Jordan	R Parkinson	

Contents

Glossary **1**

1 Introduction **2**

2 'Define' **9**

2.1 Quality Function Deployment 9

2.2 Reliability Block Diagram (RBD) 12

2.3 Reliability Allocation 14

3 'Identify' **17**

3.1 Change Point Analysis (CPA) 17

3.2 Failure Mode, Effects, & Criticality Analysis (FMECA) 20

4 'Analyse & Assess' **27**

4.1 Reliability Databases 27

4.2 Physics of Failure 29

5 'Quantify & Improve' **34**

5.1 Life Data Analysis 34

5.2 System Reliability Analysis 36

5.3 Design of Experiments 38

5.4 Fault Tree Analysis 41

5.5 Reliability Growth 45

5.6 HALT/HASS/ALT 49

6 'Validate' **53**

6.1 Reliability Demonstration Testing 53

7 'Monitor & Control' **55**

7.1 Root Cause Analysis 55

7.2 FRACAS 58

8 Recommendations for further work **63**

List of Figures

Figure 1 - Quality and Reliability Tools showing common elements 5
Figure 2 - Core Design Process with Integrated Reliability Processes and Simulation Tool 7
Figure 3 - The QFD Inputs to the Design Process 9
Figure 4 - QFD Worksheet – also known as 'House of Quality' 11
Figure 5 – Process Intensity of the Quality Function Deployment 12
Figure 6 - The Reliability Block Diagram process within the Design Process 12
Figure 7 - Process Intensity of a Reliability Block Diagram 14
Figure 8 - The Reliability Allocation Process within the Design Process 14
Figure 9 - Process Intensity of a Reliability Allocation 16
Figure 10 - Example of the CPA Process used within the Design Process (Design Iteration) 17
Figure 11 - Change Point Analysis Process Intensity 19
Figure 12 - FMECA Timings 21
Figure 13 - SADT Representation of a P Diagram 23
Figure 14 - FMECA Process Intensity 25
Figure 15 - Example of Physics of Failure process used within the Design Process (Design Iteration) 29
Figure 16 - Defining & Analysing the System for PoF 31
Figure 17 - Physics of Failure Process Intensity 32
Figure 18 - Example of Life Data & System Reliability Analysis within the Design Process (Design Iteration) 34
Figure 19 - Life Data Analysis Process Intensity 36
Figure 20 - System Reliability Analysis Process Intensity 38
Figure 21 - Process Factors & Responses 38
Figure 22 - Example of a Main Effects Plot (Example shows Temperature & Pressure) 40
Figure 23 - Design of Experiments Process Intensity 41
Figure 24 - Example of Fault Tree Analysis within the Design Process 42
Figure 25 - Simple Fault Tree showing event types 43
Figure 26 - Fault Tree Analysis Process Intensity 44
Figure 27 - Reliability Growth within the Test Phases of the Design Process 46
Figure 28 - Sample Reliability Growth Curve for a Test Fix Test programme 48

Figure 29 - Reliability Growth Process Intensity 48
Figure 30 - The scope of HALT tests extends to 'Destruct Limits'..... 50
Figure 31 - HALT/HASS/ALT Process Intensity..... 52
Figure 32 - Reliability Demonstration Testing Process Intensity..... 54
Figure 33 - Root Cause Analysis Process Intensity..... 57
Figure 34 - FRACAS process flow diagram 59
Figure 35 - FRACAS Process Intensity..... 61

List of Tables

Table 1 - Summary of Acronyms 1
Table 2 - Comparison of Tidal v Established Industries 6
Table 3 - Summary of 'Process Intensities' and Technical Report References 8
Table 4 - Changed Part Codes 18
Table 5 - Attribute Change Codes 18
Table 6 - Example of a CPA Worksheet 19
Table 7 - Qualitative Risk Rankings – FMECA 24
Table 8 - Key Requirements for a Tidal Turbine Reliability Database 28

Glossary

Table 1 below shows a complete summary of acronyms used within the body of the report.

Acronym	Full title
(D or P) FMEA	(Design or Process) Failure Mode and Effects Analysis
ALT	Accelerated Life Test
ARINC	Aeronautical Radio Incorporated
CM	Condition Monitoring
CPA	Change Point Analysis
DfR	Design for Reliability
DoE	Design of Experiments
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis and Corrective Action System
FTA	Fault Tree Analysis
HALT	Highly Accelerated Life Test
HASS	Highly Accelerated Stress Screen
HATT	Horizontal Axis Tidal Turbine
MTBF	Mean Time Before Failure
MTTF	Mean Time To Failure
NDT	Non-Destructive Test(ing)
PDS	Product Design Specification
PoF	Physics of Failure
QFD	Quality Function Deployment
RBD	Reliability Block Diagram
RCA	Root Cause Analysis
RDT	Reliability Demonstration Testing
RG	Reliability Growth
TiPTORS	**Ti**dal **P**ower **T**ake **O**ff **R**eliability **S**imulation
WT	Wind Turbine

Table 1 - Summary of Acronyms

1 Introduction

This report is a technical summary of the work carried out to develop a Design for Reliability (DfR) process, focused specifically on Tidal Turbine devices. The body of work comprises Phase 1 of the Tidal Power Take Off Reliability Simulation (TiPTORS) collaboration agreement between Offshore Renewable Energy Catapult and Ricardo UK.

The DfR process has a number of key objectives;

- It can be applied to a wide range of Horizontal Axis Tidal Turbine devices.
- It can be easily integrated alongside any Design Process.
- Elements of the process can be used effectively as stand-alone tools.
- Most processes already exist within other industries and are supported with extensive literature on their application.

The DfR methodology will be further enhanced by the creation of a Design Simulation Tool, developed by DNV GL who are also part of the collaborative group in Phase 1. Details of the Simulation Tool are given in a separate report (PP124801-WP1.5-001).

A flow chart of the DfR methodology and Simulation Tool aligned with a generic Design Process is shown in Figure 2

All of the processes briefly described within this report are supported by more detailed technical reports on the individual subjects. These individual reports also provide details of further literature in their Reference and Bibliography sections to assist the practitioner. A list of these reports is given in Table 3.

The structure adopted for the DfR methodology is divided into six groups which reflect the stages of a product development cycle and its associated reliability, from setting reliability targets through to reliability demonstration. These groups are defined as:

- Define
- Identify
- Analyse & Assess
- Quantify & Improve
- Validate
- Monitor & Control

The above headings are used in this report to discuss the individual processes within each of them.

Within each section, the processes are described in summary by their objective or purpose, how the process is approached and the expected results or benefits. An attempt is also made to give the process user an idea of the effort that may be required to successfully execute each process. This is termed “Process Intensity”. It gives a subjective rating (on a scale of 1 to 4) of the following process attributes:

- Cost
- Resource
- Complexity

Additionally, some guidance is also given in terms of whether a specific process is essential, or otherwise, within the overall DfR process. Each process has a further rating as follows:

- Essential
- Recommended
- Optional

It is recognised that Tidal Turbine devices are not yet in full scale commercial operation as arrays, working in tidal streams and delivering a commercially acceptable cost of energy.

It is also recognised that a variety of solutions (architectures) exist as prototypes and experimental devices in the water.

The current state of Tidal Turbine development means there is a lack of basic “legacy” data in the industry, particularly reliability data, making the adoption of some of these processes challenging. It is expected that during the early phases of designing Tidal Turbine devices to a system reliability target that estimates will have to be used extensively. These reliability estimates will form the basis of early models in Reliability Block Diagrams and other models. Within the processes, some of these estimated values may be traded against other parts in a balancing act to achieve a target system reliability. In other cases, real data may become available to replace the estimate, thus increasing the accuracy of models. It might be necessary to introduce redundancy into the design or even a different design or technology to help achieve a reliability target.

When all of the above has been processed, there will remain some “inviolable” reliability requirements that cannot be assigned elsewhere or compromised. These will in fact become “targets” which will have to be met by supplier or developer.

This element of the DfR process which drives credible reliability targets is a key enabler for any Tidal Developer as it provides real data with which to drive reliability requirements into the

supplier base as well as internal processes. With this data, reliability targets can be enforced with confidence.

Some of the processes within the DfR methodology will require a high level of knowledge of statistical techniques in order to fully understand aspects of reliability such as the application of correct failure distributions to components/sub-systems and models, censored data etc. These skills are also key to the correct interpretation of analytical and test results to ensure correct decisions are made downstream. This applies in particular to Reliability Growth tracking which is considered the most technically complex task to undertake within the DfR suite of processes.

As well a technical competence, it is equally important to ensure that adequate budgets are allocated for processes to be undertaken correctly.

Another enabler for this process, not covered in Phase 1, is the development of a cost model against which any reliability improvements, either to meet or exceed targets, can be evaluated. These models will be unique to the Tidal Developer and reflect the organisations costing structure. It is however an essential tool to ensure the correct (long term) value is assigned to any changes that affect costs. Any model must recognise the cost of failures in the field, including contractual penalties, as a balance against any process or product cost increase. The model should also be capable of looking at any offsets that are available to mitigate on-costs.

It must not be assumed that a Quality Operating System will deliver Reliability in a product. While both processes share common tools (see Figure 1), their objectives are different:

QUALITY: Is a measure of compliance to a drawing or specification and ultimately a design. If the part conforms to the specification then it is said to have achieved the required quality level. The process does not interrogate a design for intended function.

RELIABILITY: Is a function of a design (assuming it is made to specification). It is a measure of a component or system’s ability to deliver an intended function repeatedly over a specified time, number of cycles or distance.

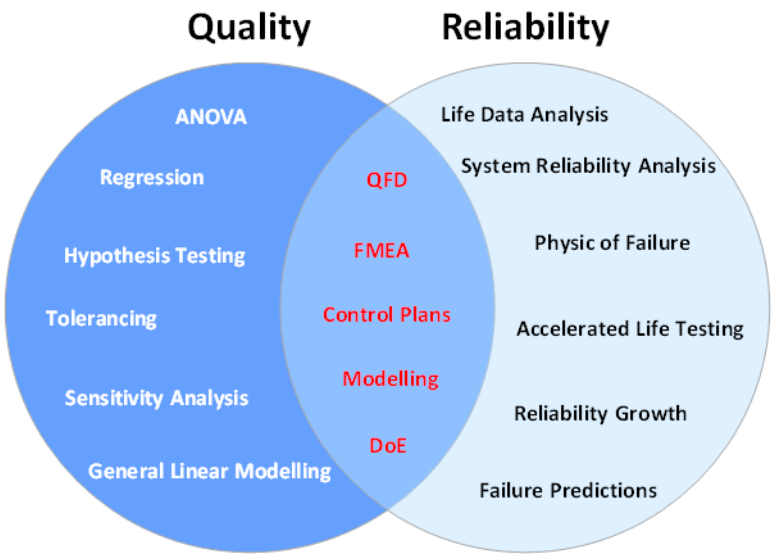

Figure 1 - Quality and Reliability Tools showing common elements

Looking forward towards Marine Energy Converter Certification schemes, the basis for certification will inevitably document reliability targets, along with functional safety and environmental targets. It will also describe the operating conditions and design survival conditions for the device.

The relative immaturity of the Tidal Turbine Sector brings challenges, principally regarding their performance against more traditional and established energy producers. Despite the adoption of selected carry over components from more established industries such as Hydro power, power generation, shipping etc., the application specific adjustments (duty cycles, mission times and operating environment) can bring challenges similar to those for new components and systems.

Any environmental benefits of such systems will easily be outweighed if they are unable to deliver energy with acceptable levels of Reliability, Availability & Maintainability. The case for adopting Design for Reliability processes is very strong in an industry that needs to demonstrate performance and commercial equality with other systems in a very short time period. Table 2 below highlights some of the challenges:

Established Industries	Tidal Turbines
Established product development processes	Processes still being "optimised" for the product.
Generally (but not always) higher sample sizes available	Very often single prototypes
Reliability targets driven by customer satisfaction	Reliability driven by financial penalties
High levels of historical product data	Low levels of product data
Mature supplier base	New supplier base (for application)
Convergence of designs / architectures to perform a function (natural selection)	Diversity of designs (some will prove less able than others with time)
Established cost models	Cost models to be or being developed

Table 2 - Comparison of Tidal v Established Industries

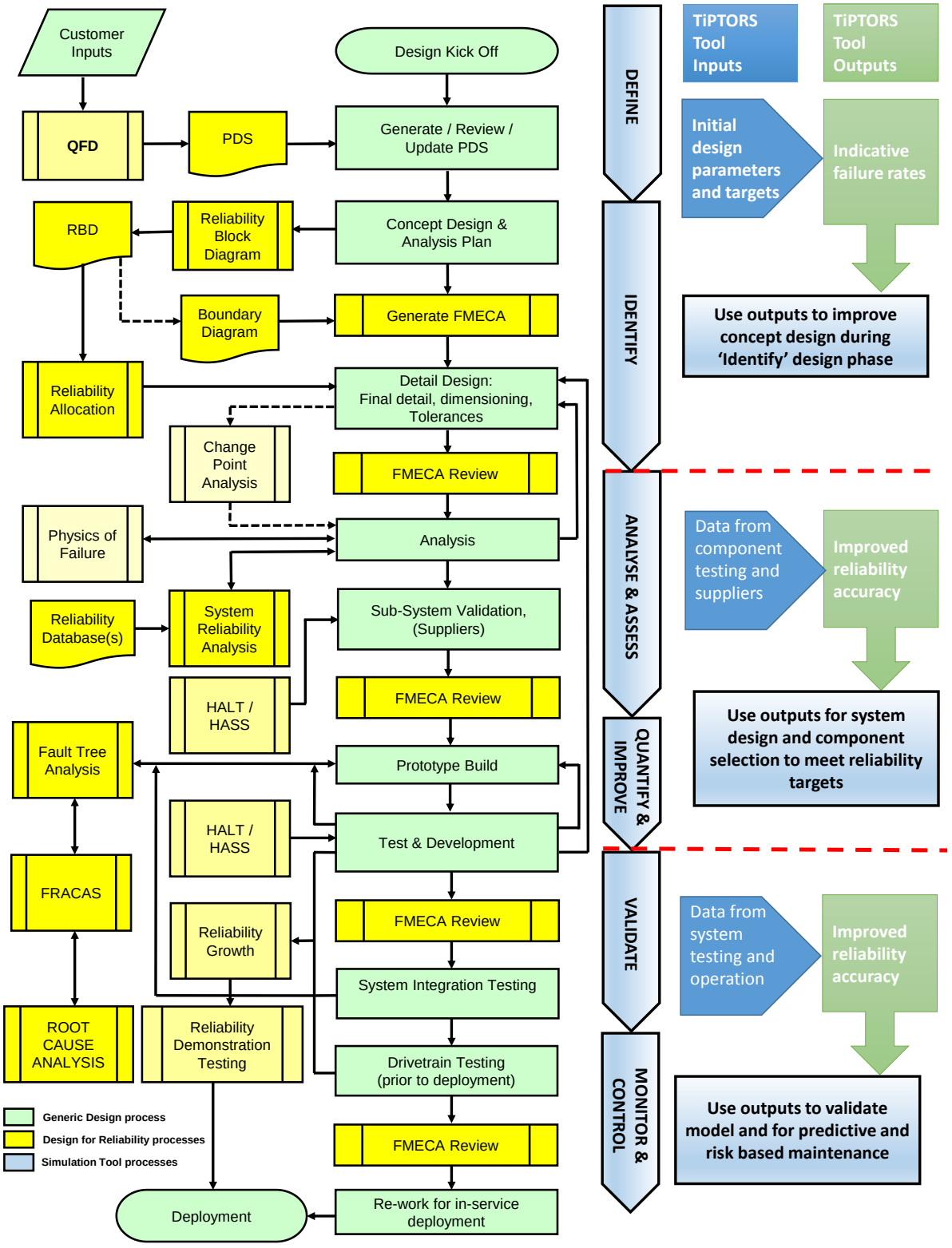

Figure 2 - Core Design Process with Integrated Reliability Processes and Simulation Tool

The Design Process shown, in green, is "generic" and will tend to differ in detail between companies.

For further information on these processes refer to:

BS7000: Design Management Systems

BS8887: Design for Manufacture

BS5760: Design for Reliability

Process	Cost	Resource	Complexity	Applicable	Technical Report Reference
DEFINE					
Quality Function Deployment	2	2	1	Recommended	RD.15/000418-1
Reliability Block Diagram	2	2	2	Essential	RD.15/91101.1
Reliability Allocation	2	3	2	Essential	RD.15/82201.1
IDENTIFY	2				
Change Point Analysis	1	2	1	Optional	RD.15/000517-1
FMECA	3	3	2	Essential	RD.15/104101.1
ANALYSE & ASSESS	2				
Reliability Databases					RD.15/75701.1
Physics of Failure & Condition Monitoring	3	3	3	Recommended	RD.15/141601.1
QUANTIFY & IMPROVE					
Life Data Analysis	3	2	3	Essential	RD.15/001038.1
System Reliability Analysis	2	2	2	Essential	RD.15/001038.1
Design of Experiments	3	2	3	Recommended	RD.15/001027-1
Fault Tree Analysis	2	2	2	Recommended	RD.15/001035-1
Reliability Growth	4	3	4	Essential	RD.15/001048.1
HALT / HASS /ALT	2	2	3	Recommended	RD.15/001168.1
VALIDATE	3				
Reliability Demonstration Testing	4	3	4	Recommended	RD.15/001048.1
MONITOR & CONTROL					
Root Cause Analysis	2	1	2	Recommended	RD.15/000834-1
FRACAS	3	3	2	Essential	RD.15/000875.1

Table 3 - Summary of 'Process Intensities' and Technical Report References

The numbers quoted for Cost, Resource and Complexity for each process are estimates, expressed as relative rankings on a scale of 1 to 4.

The rankings may require some revisions following the application and execution of these processes.

2 'Define'

2.1 Quality Function Deployment

2.1.1 Objective

This really is the start of the Design for Reliability process. Until you know what is required of a Tidal Turbine you cannot set about designing it.

Quality Function Deployment is a process used by many organisations to capture the requirements of their customers and translate these into a set of technical requirements for the product being proposed. Figure 3 shows when the QFD process should be started within the Design Process.

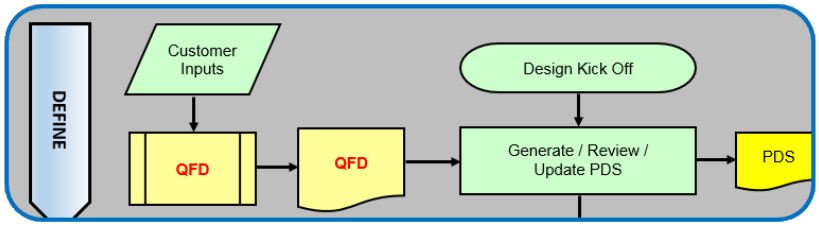

Figure 3 - The QFD Inputs to the Design Process

In theory, the successful implementation of all the technical requirements will meet the cost, reliability, quality, serviceability, performance, legislative, environmental requirements etc. of the customer.

Find out what the customer really wants. (Sometimes the customer may not be clear on requirements!)

Engage with the customer and "brainstorm" all the requirements the product must meet:

- *Technical*
- *Commercial*
- *Legislative*
- *Environmental*

2.1.2 Activities

The process can be executed at a pre-contract stage where all requirements may not be fully understood, developed or even known. Once completed, the information can be used not only

to develop an accurate Technical Specification but also provide a more accurate model for contractual costing.

The customer's requirements form the basis for defining the product specification so it is important that these are accurately recorded and understood. They are best defined by the customer, and it can be useful to let the customer describe them in their own words.

Customer tenders and Product Definition Specifications are the principle source of requirements, along with any regulations applying to the sector in question. They are often a source of friction or disagreement between a supplier and customer, and it is therefore important that requirements are fully understood at this early stage and agreed by both parties in any contracts.

Additional customer requirements can be captured using questionnaires and interviews for example. Detailed verbal and written descriptions from the customer which are then converted into statements, should accurately fill any gaps that exist in the information on customer needs.

A weighting is generally applied to Customer Requirements in order to generate results which are clearly 'ranked' in order of importance.

Don't rely on the customer knowing every requirement. If Tidal Turbines is your field of expertise, you may know some of the requirements better than the customer.

Consider using a technical questionnaire for the gathering of information (the questions can be structured to ensure the correct information is provided)

The chart used to collect the inputs, process the data and display the output of QFD is commonly known within industry as the "House of Quality" and a sample worksheet is shown in Figure 4 below

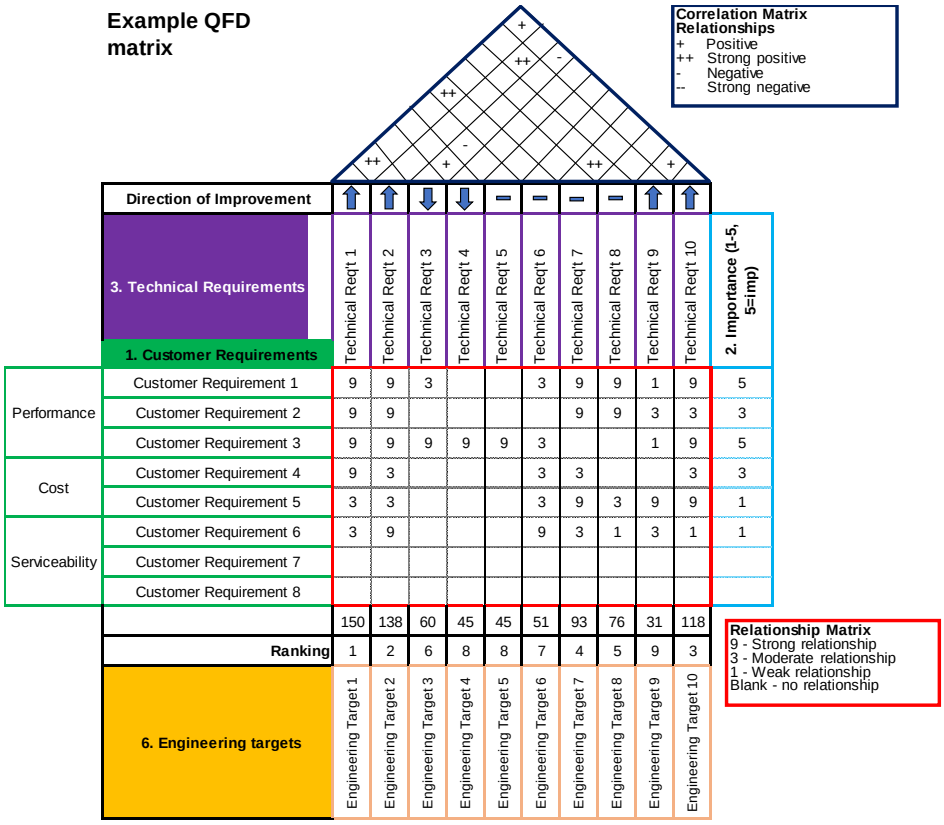

Figure 4 - QFD Worksheet – also known as 'House of Quality'

Details and instructions on how to perform the full QFD process are given in Report **RD.15/000418-1**: *Quality Function Deployment.*

Use "competitive benchmarking" information as another source of requirements. If your customer doesn't have a clear idea of a requirement then their competitor might!

2.1.3 Deliverables

The output from the process will be a set of Engineering Specifications which have been derived from the Customer Requirements. Within the process, some trade-offs may be required where requirements conflict. These trade-offs are also processed within the Correlation Matrix embedded within the QFD matrix.

2.1.4 Process Intensity

The amount of input required to produce the Quality Function Deployment in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 5 below;

Figure 5 – Process Intensity of the Quality Function Deployment

2.1.5 QFD Checklist

- ✓ All customer requirements are fully understood by the supplier.
- ✓ Supplier has discussed any ambiguous requirements with customer and resolved them.
- ✓ All customer requirements have been recorded and grouped.
- ✓ Customer requirements have been allocated an “importance” weighting.
- ✓ Have all “trade-offs” been considered and associated risks evaluated?

2.1.6 Further Reading

RD.15/000418-1: *Quality Function Deployment*

2.2 Reliability Block Diagram (RBD)

2.2.1 Objective

Before Reliability Analysis can be performed on a Tidal Turbine System, the operational relationships of the sub-systems and components must be known. This is usually defined (in its first iteration) at the Concept Design stage. A Reliability Block Diagram (RBD) is a graphical representation of how the components or sub-systems within a system are connected to provide a desired outcome, often referred to as “system or mission success”

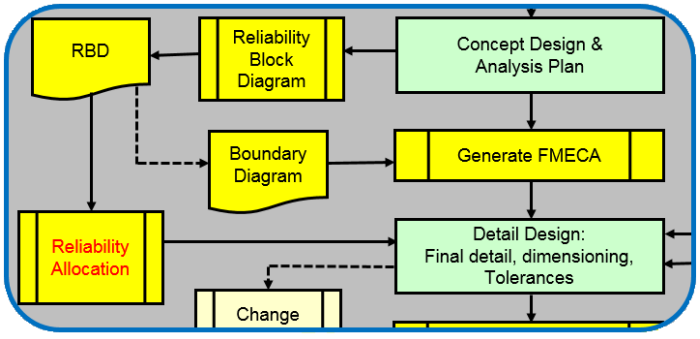

Figure 6 - The Reliability Block Diagram process within the Design Process

A Reliability Block Diagram will also double as the basis for the Boundary Diagram in the FMECA

Early work in the design process with RBD's will yield useful data at the Tidal Turbine design stage to determine the ability of intended systems, sub-systems, and components, to meet reliability targets within the devices.

2.2.2 Activities

The outline process steps to create an RBD are:

- Define the boundary of the system to be analysed.
- Break the system into functional components.
- Determine series – parallel combinations or groups.
- Represent each component or sub-system as a separate block.
- Connect each block by lines in a logical order for correct function of the system.

Break the system into its most basic parts. See if complex structures can be reduced to "series" and "parallel" sub-systems

---

Where specific Tidal Turbine designs are being considered, more complex configurations (mixed series and parallel) may be encountered. These must be considered individually, based on their structure. However, the vast majority of systems can be covered by either series or parallel structures.

Report **RD.15/91101.1**: *Initial Reliability Block Diagram Algebraic Structure* covers construction of RBD's, series and parallel systems, and also discusses the characteristics of components in terms of failure modes, distributions & independent failures, and repairable & non-repairable systems in greater detail.

2.2.3 Deliverables

Once a Reliability Block Diagram has been generated and the algebraic relationships between components in a sub-system are defined, this structure is used to evaluate the effects of Reliability Allocation (described in 2.3 below) for sub-systems/components on the reliability of the total system.

2.2.4 Process Intensity

The amount of input required to produce a Reliability Block Diagram in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 7 below;

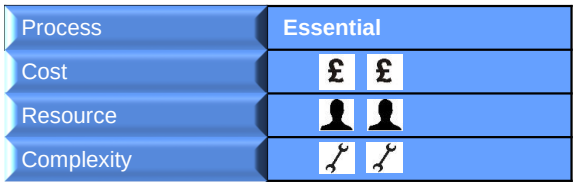

Figure 7 - Process Intensity of a Reliability Block Diagram

2.2.5 Reliability Block Diagram Checklist

- ✓ Have all components or sub-systems been included within the boundary?
- ✓ Failure Rates – Have correct distributions been defined?
- ✓ Are all failures “independent” – have system interactions been considered?
- ✓ Have Repairable / Non-repairable systems been defined?
- ✓ Have all system interrelationships been correctly defined?
- ✓ Have any components with more than one failure mode been identified?

Note: If a component has two discrete failure modes (e.g. fail open & fail closed) have both been considered?

2.2.6 Further Reading

RD.15/91101.1 : Initial Reliability Block Diagram Algebraic Structure.

2.3 Reliability Allocation

2.3.1 Objective

One of the essential criterion of a Design for Reliability (DfR) program for Tidal Turbines is defining the reliability goals that the device needs to achieve. Reliability Allocation is a process for apportioning a system target reliability amongst sub-systems and components. It is an essential tool at the design stage for determining the required reliability of equipment to achieve a reliability target for a given system, in this case a Tidal Turbine.

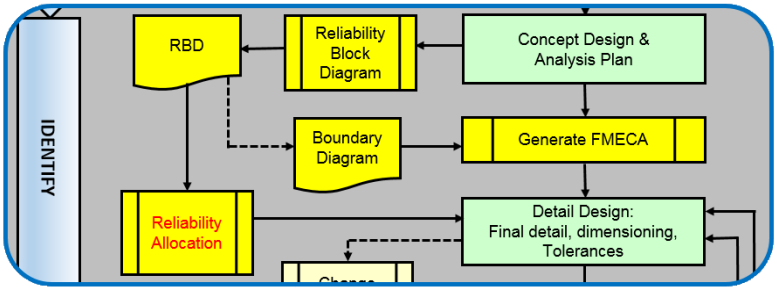

Figure 8 - The Reliability Allocation Process within the Design Process

This involves a balancing act in order to determine how to allocate reliability among the sub-systems and components.

Reliability targets at component level are essential at the "Define" stage of the programme to ensure reliability targets are known and correctly specified prior to sourcing.

"It is extremely difficult to increase the reliability of an existing part retrospectively without affecting other components..."

The reliability targets for each component or sub-system are fed back into the RBD, discussed above, to yield the system reliability target.

2.3.2 Activities

During Phase 1 of the TiPTOR's Programme, three processes were investigated for use within the Design for Reliability process and Simulation Model for Tidal Turbines.

2.3.2.1 Equal Apportionment

Based on the assumption that the same reliability target is assigned to each sub-system or component, its weakness is that the sub-system goals are not assigned in accordance with the degree of difficulty associated with achieving them for each sub-system or component type.

2.3.2.2 ARINC

The ARINC process applies weightings to the sub-system/component reliability targets to reflect the different reliability performances of different sub-system types. This process will yield a more accurate measure of the required sub-system reliability goals than Equal Apportionment. For early concept stage studies and estimates, the ARINC process may be employed as this does provide some recognition of sub-system differences in reliability through its weighting process.

2.3.2.3 Feasibility of Objectives Technique

The Feasibility of Objectives process considers four "real world" rating criteria for the weighting and application of reliability targets.

- System Complexity
- State-of-the-Art (Technology)
- Performance Time
- Environment

Worked examples of all three processes and how to execute them plus further reference material can be found in report: **RD.15/82201.1** – *Reliability Allocation Process for Horizontal Axis Tidal Turbines.*

2.3.3 Deliverables

The Feasibility of Objectives Technique will ultimately yield greater accuracy of reliability estimation and apportionment and it is recommended for use in the Tidal Turbine DfR methodology and Simulation Tool. The use of a suitably qualified engineering team with knowledge of the sub-systems is key to the success of this process.

2.3.4 Process Intensity

The amount of input required to produce a Reliability Allocation in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 9 below;

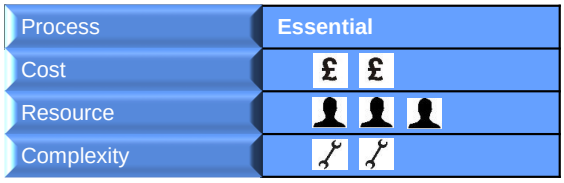

Figure 9 - Process Intensity of a Reliability Allocation

2.3.5 Reliability Allocation Checklist

- ✓ Has a realistic reliability objective or target been defined for the device (system)?
- ✓ Is there sufficient knowledge of the sub-systems within the device in terms of their predicted reliability?
- ✓ Has complexity, technology used, performance time and operating environment been considered for each component/sub-system
- ✓ Have any relevant reliability databases been interrogated for reliability values?
- ✓ Has historical reliability performance data from existing components / sub-system devices been considered?

2.3.6 Further Reading

RD.15/82201.1 : Reliability Allocation Process for Horizontal Axis Tidal Turbines

3 'Identify'

3.1 Change Point Analysis (CPA)

3.1.1 Objective

CPA is used to help understand the levels of change from earlier designs (if applicable) or evaluate the risk associated with design changes when undertaking for example, Reliability Growth tracking. With a "clean sheet" design, this process will not generally be required; but during development phases, design iterations, particularly those associated with Reliability Growth, these processes will benefit from using Change Point Analysis.

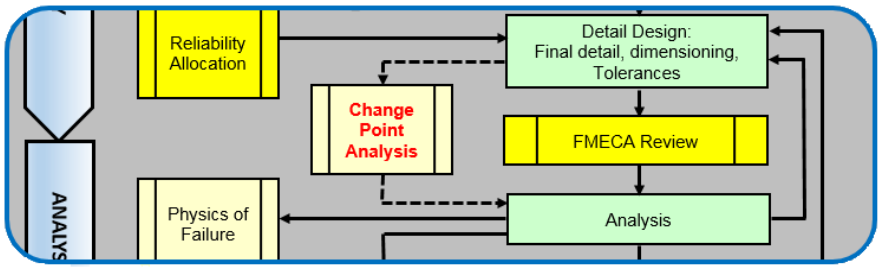

Figure 10 - Example of the CPA Process used within the Design Process (Design Iteration)

CPA assesses how much has changed, the nature of the changes, and subjectively, the risk associated with those changes.

It is not intended to objectively evaluate and mitigate risks but to ensure:

1. The risk is identified.
2. The risk is considered within the appropriate DfR or Quality process (e.g. FMECA, Test Plan) to objectively evaluate and mitigate any effects.

Adopt the philosophy that "there is no such thing as a carryover part!"

Even a tried and trusted component applied to a different product is exposed to new failure risks…

For this process to work, it is essential that drawing changes are identifiable by drawing "up-issue" when part numbers do not change. If not then changes can be missed!

3.1.2 Activities

CPA should be undertaken by a multi-disciplined team including representatives from Engineering, Quality, Purchasing and Manufacturing.

The importance of Change Point Analysis is that, firstly, the team can identify areas of greatest risk to their part of the system. Secondly, the process helps to focus the activities of engineering personnel, the use of resources and enables the prioritisation of changes with all potential concerns.

The process starts by identifying changes between the proposed and existing products, usually through comparison of their respective Bills of Material (BOM's). The first three columns in Table 6 shows how this might look.

Once changes to components have been identified, the types of change applicable to each is defined using a two part code which describes the status of the new part with respect to the existing part and a description of the attribute that has changed. See Table 4 & Table 5

With the point of change and type of change identified, the risk is then assessed. This should be done in a discussion/workshop environment with inputs from a cross-functional team to bring expertise from their various disciplines.

There are several aspects to evaluating the risks:

- Identifying the concerns and/or impacts of the change
- Allocating a risk level score (normally H, M, L as process is subjective)
- Justifying the reason for the score.
- Identifying a mitigation strategy for reducing the risk

All of the above aspects of the risk are recorded in Table 6 below and the appropriate actions listed to eliminate or mitigate the risk. This will often be carried out through other DfR or Quality processes such a FMECA.

It should be remembered that carry-over parts which are being sourced from a different supplier also constitute a risk which should be suitably managed. It should not be assumed that this type of change will always be identified and appropriately managed under the Quality System.

Change Description Summary	
Carry over part	CP
New part	NP
Carry over Modified part	CMP [Attribute Change(s)]
Deleted part	DP

Table 4 - Changed Part Codes

Change Description Attribute	
Material	M
Geometry	G
Heat Treatment	HT
Finish	F
Process	P
Supplier	S

Table 5 - Attribute Change Codes

The Change Descriptions in Tables 4 & 5 are not definitive. Other attributes should be used if appropriate.

Identify the Change			Evaluate the Risks				
Part Description	Existing Assy	New Assy	Change Description Summary	Concerns / Impacts	Risk Priority	Priority Reason	Risk reduction strategy for HP Items
Hub	Existing part	Existing part	CP	None	L		
Position Sensor	Existing part	Existing part	CP	High failure rate	H	Concern with existing sensor	Supplier
Ring Gear	Existing part	New part	NP	Torque path part	H		
Planet Pin	Existing part	New part	CMP[M, G, S]	Lubrication	H	Critical	Lube Test
Sun Gear	Existing part	New part	CMP[G]		M	Minor geometry change	DV Test
Oil Seal	Existing part	Existing part	CP	None	L	C/over conditions	
Input Shaft	Existing part	New part	NP + [S]	Torque path part	H	New part &new supplier	DV Testing & ISIR

Table 6 - Example of a CPA Worksheet

3.1.3 Deliverables

The CPA process will deliver risk mitigation (and elimination) activities for all components undergoing change through activities such as product design phases, test phases, root cause analysis actions etc. It allows early definition and understanding of the implications of a change. In many cases, changes are considered at the point of entry into a later process and may not always be given due consideration due to time pressures or the magnitude of components to be considered.

3.1.4 Process Intensity

The amount of input required to produce a Change Point Analysis in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 11 below;

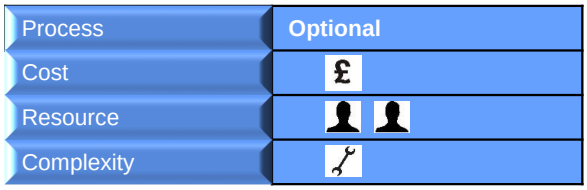

Figure 11 - Change Point Analysis Process Intensity

3.1.5 Change Point Analysis Checklist

✓ Has the CPA been conducted with a suitably qualified multi-disciplined team?

- ✓ Have all changes have been identified for the level of design being considered?
- ✓ Have all changes been allocated their true Change Description Codes?
- ✓ Ensure any supplier changes for Carry Over parts have been captured as risks?
- ✓ Have Risk Reduction Strategies been identified for all High and Medium Risks?

Don't overlook existing parts which are to be made by a different supplier – this also represents "change"!

3.1.6 Further Reading

RD.15/000517-1 – Change Point Analysis Process

3.2 Failure Mode, Effects, & Criticality Analysis (FMECA)

3.2.1 Objective

Failure Mode and Effects Analysis (FMEA) is a qualitative reliability technique for systematically analysing each possible failure mode within a hardware system, and identifying the resulting effect on that system, the mission and personnel.

Criticality Analysis (CA) is a quantitative procedure which ranks failure modes according to their probability and consequences (i.e. the resulting effect of the failure mode on system, mission or personnel).

The combination of the above two processes is referred to as a Failure Mode & Effect and Criticality Analysis (FMECA).

The processes can be implemented using a functional (top down) approach or a component (bottom up) approach. This report recommends a "component" approach to FMECA analysis as this is better suited to align with individual component performance, reliability objectives and targets. The process is suited to examine hardware, firmware, software and human elements of Tidal Turbine Systems.

Design FMEA and Process FMEA are often used in conjunction to ensure that the design meets the requirements, risks are understood and that the manufacturing process (assembly and installation included) is capable of meeting the design intent.

The FMECA is a "living document" in the DfR process. It needs to be updated as information changes in order to reflect the current status of a design.

3.2.2 Activities

The approach adopted for the FMECA process, is based partly on that described in **MIL-STD-1629A** and processes developed by **DNV GL** and adopted across the Wind Turbine and Offshore industries.

An FMECA should be incorporated as an integral part of the Design for Reliability process from preliminary or concept design through to the final design as illustrated in Figure 12. The document should be regularly updated to capture design changes, feedback from analysis, feedback from testing and the refinement of any reliability data generated throughout the programme. The FMECA should always reflect current design and current reliability/failure data. While the reader will probably be familiar with DFMEA or FMECA basic techniques, some aspects of the FMECA applicable to Tidal Turbines are stated below.

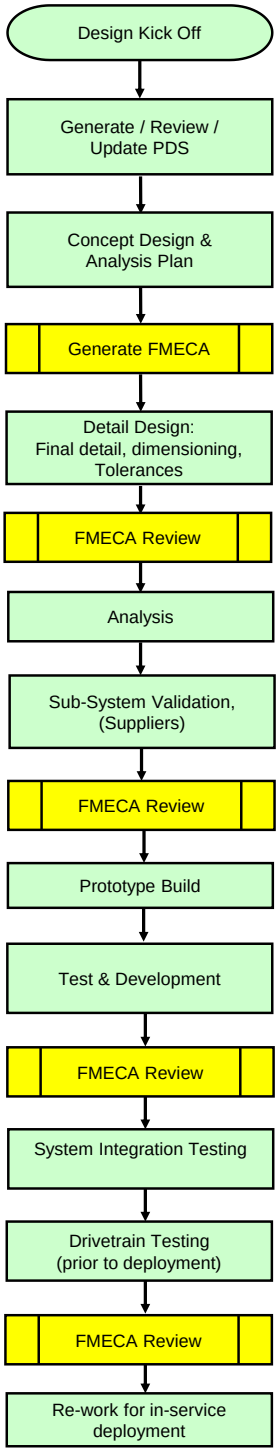

Figure 12 - FMECA Timings

3.2.2.1 The FMECA Team

The FMECA team should include the following:

FMECA facilitator | System Design Engineer | Component Design Engineer | Development Engineer | Quality Engineer | Analyst | Reliability Engineer.

For meetings to be effective, there should be a minimum of 3 competent people in any FMECA meeting. If a key team member is unavailable for a specific meeting, the meeting should be re-scheduled to assure quality and validity of important decisions.

3.2.2.2 Boundary Diagram

A Boundary Diagram is used in the preliminary stage of an FMECA (and other Design for Reliability processes) to:

- Identify all the elements within a sub-system in their functional positions and configurations.
- Identify which sub-systems or components influence the operation, interrelation and interdependencies of the system within the boundary of the system and define the boundary

The construction of a Boundary Diagram is explained in greater detail in Report RD.15/104101.1 -FMECA Guide Tool for Tidal Turbines. However, there are some guidelines which should be adopted for all Boundary Diagrams constructed for Tidal Turbine FMECA's.

1. A logical numbering system should be adopted and used for each element to enable traceability and tracking throughout the process, and beyond. This will allow easy identification of any component within its sub-system and be consistent with numbering systems used elsewhere in the DfR process, for example Reliability Block Diagrams (RBD's). The adoption of a universal numbering system will also help where FMECA's are carried out at different levels within the same system. It is recommended that the numbering system and system partitioning developed by DNV GL and referenced in report **RD.15/78801.1** - *Definition of System Architecture of Horizontal Axis Tidal Turbine* (HATT) is adopted for Tidal Turbine Boundary Diagrams and their associated FMECA's.
2. A consistent legend should be adopted for all interface types, regardless of the system being investigated (e.g. Mechanical, Electrical, Hydraulic) within the Tidal Turbine. This will assist when looking at interfaces which span two or more sub-systems.

Note: The adoption of a standard Taxonomy and Numbering will help in the creation of a Tidal Turbine Reliability Database.

3.2.2.3 Function Tree

To ensure all the functions of the system are correctly identified, a Function Tree is generated. This should be carried out by the full FMECA team following the process described in outline below:

- Using the Block Diagram, identify, by brainstorming, the hierarchical functions of the system being investigated. These are the high level or primary functions and collectively represent what the component or sub-system is supposed to do.
- . Using the generated list of highest level functions, consider the sub-functions which achieve the primary function. This can be done by asking "how is the function achieved"
- Continue to "drill-down" into the lower level functions and their own supporting functions which support the higher level until the lowest function is identified.
- Each of the primary functions may have a different number of sub-functions below them

It should be ensured that all the functionality of higher functions are covered by the lower level functions.

3.2.2.4 Parameter Diagram

The Parameter Diagram (P-Diagram) takes the inputs to a system and relates those to desired outputs of the system under investigation. It also considers non-controllable outside influences on the function of the system. The P-Diagram, is an essential tool for brainstorming and documenting the following prior to starting an FMECA and comprises:

Input signals

- Ideal Outputs
- Control Factors
- Noise Factors
- Error States (or failure modes)

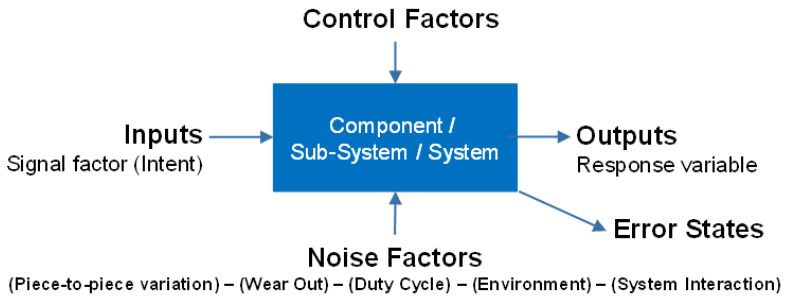

Figure 13 - SADT Representation of a P Diagram

Note: A "P" Diagram will enable all noise factors to be identified for a system which should be included in all testing.

3.2.2.5 FMECA Document

An example of the complete FMECA document format is shown in report **RD.15/104101.1** - *FMECA Guide Tool for Tidal Turbines.*

The following sections should be included within the FMECA worksheet and be populated by the team based on the guidelines given in the above report:

- Component & Identifier
- Function
- Technical Class
- Novelty
- Failure Mode
- Failure Mechanism or Cause
- Key Indicator
- Prevention Control

- Detection
- Consequences
- Current Controls
- Ranking of Risks
- Consequence
- Probability
- Risk Categories
- Recommended Actions, Responsibility & Review

Within the FMECA, it should be assumed that the components will be manufactured and assembled correctly to drawing, within the limits of expected process variation.

3.2.2.6 Criticality Analysis

While the FMECA analyses different failure modes and their effect on the system, the Criticality Analysis (CA) classifies and prioritises their level of importance based on Consequence of the effect and Probability of failure. Table 7 below shows the qualitative rankings of risks based on these.

	Consequence				
Prob.	**1**	**2**	**3**	**4**	**5**
5	Low	Med	High	High	High
4	Low	Med	Med	High	High
3	Low	Low	Med	Med	High
2	Low	Low	Low	Med	Med
1	Low	Low	Low	Low	Med

Table 7 - Qualitative Risk Rankings – FMECA

Note: FMECA's for large systems such as Tidal Turbines should be approached by dividing into appropriate sub-systems for ease of management and better attention to detail.

Where failure rates, failure modes, failure mode ratios and failure effect probabilities are available, a quantitative method may be used and this is discussed in more detail in report **RD.15/104101.1** However, the data required to complete a quantitative risk analysis is not readily available at present for Tidal Turbine devices.

As parts and failure rate data become available as the system matures, it will be possible to calculate criticality numbers and incorporate them into the rankings and analysis.

A shortcoming of qualitative criticality ranking is the inability to allow the engineer to identify high risk or Consequences of failure simply from the product of Consequence and Probability. It is possible that two or more failure modes may have similar numbers as they are the product of Consequence and Probability, *but one may have a much higher severity or Consequence of failure.*

3.2.3 Deliverables

FMECA's can be time consuming and require additional resources to be completed successfully. The processes summarised in this report highlight the level of additional effort that is required to complete Criticality Analysis over and above an FMEA.

The target lifetimes and extended maintenance periods, together with the costs associated with retrieval of a Tidal Turbine device due to a system or component failure demand similar levels of equipment reliability and availability as most key defence equipment. The financial consequences of a system failure due to a seal or a generator are very similar when retrieval costs comprise a major part of the total cost of repair.

FMECA will provide key information on all parts within the system in terms of failure risks. In many cases, with the lack of reliability data, this will be qualitative but as knowledge of failure rates increases with testing and service activities, this will be displaced with more quantitative data, resulting in a greater accuracy in predictions of failures.

3.2.4 Process Intensity

The amount of input required to produce a FMECA in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 14 below

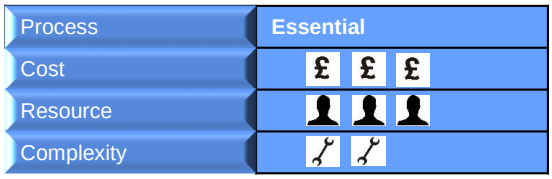

Figure 14 - FMECA Process Intensity

3.2.5 FMECA Checklist

- ✓ Has a suitably qualified team been assigned to the FMECA?
- ✓ Has all preliminary information been assembled and pre-FMECA tasks been completed before FMECA is started?
- ✓ Have all possible failure modes been considered for a component?
- ✓ Have the correct failure mechanisms been considered?

- ✓ Have “noise” factors been considered when considering failure mechanism or cause?
- ✓ Is “estimated failure rate” data easily identifiable as such within the FMECA?
- ✓ Have all “Recommended Actions” been allocated to a responsible team member?
- ✓ Have all “FMECA Reviews” been planned for later stages in the programme?

3.2.6 Further Reading

RD.15/104101.1 - FMECA Guide Tool for Tidal Turbines.

4 'Analyse & Assess'

4.1 Reliability Databases

As part of the TiPTORS Phase 1 project, a comprehensive review has been undertaken of Reliability Databases that exist within various industries. The full details of this study can be found in report RD.15/75701.1 – Review of Reliability Databases in the Automotive, Off-Highway, Defence, Aerospace, Wind, Oil & Gas and Tidal industries.

With the exception of power electronics and controls, little data that is directly relevant to Tidal Turbine reliability is available in the public domain. For initial reliability predictions of mechanical systems, relevant sections of the Handbook of Reliability Prediction Procedures for Mechanical Equipment, published by the US Naval Surface Warfare Centre (NSWC) may be of early use in reliability predictions and allocations. This publication, referenced in report **RD.15/75701.1** is readily available for use in the public domain.

The reliability reporting systems used in the wind industry appear to be the most suitable to be adopted for Tidal Turbines. In addition, their technologies are closely aligned. This however should not exclude the study and adoption of any best practices used elsewhere in other industries, for example marine or hydro. The above report makes recommendations for putting into place, the basis for a Tidal Turbine industry wide Database. Table 8 below is a summary of the conditions that prevail within the industry and how these would need to change in order to establish an effective Tidal Turbine database.

Existing	Proposed
Individual Turbine Developers & Local Supplier Base work individually.	Working group of partner Turbine Developers & Supplier members led by industry sponsor/champion. Such a group would require convincing of tangible benefits for them to participate.
No requirement to share failure data. Concerns over identification of individual failures being identified against specific Tidal Devices. Concerns over commercial / IP disclosures.	Condition of membership. Investigate mechanisms to make data anonymous or adopt structure similar to Boeing where developer data is "screened" from other developers.
No common parts descriptions. Same component will have a different names or conversely, parts with similar names will be physically different.	Common Turbine Taxonomy. Could be enforced on the data base using forced field entry of "standard" nouns from a menu. Agreement required on Turbine architectures that are relevant to the database
Different definitions of Reliability amongst developers.	Standard definition of Reliability
Variations in what information is recorded for a failure.	Evaluate and adopt if suitable, current protocol as used by Reliawind or Sparta

Existing	Proposed
Different levels of “root cause” analysis carried out. This can range from subjective judgements about failures through to robust analysis. Difficult to determine if failure descriptions are always accurate.	Robust and consistent “Root cause analysis” process in place and used across the industry. FRACAS would provide this.

Table 8 - Key Requirements for a Tidal Turbine Reliability Database

The recommendations from this industry wide review of reliability databases is;

- A working industry group comprising Tidal Turbine Developers & Supplier members is established to enable the creation of a reliability database specifically to meet the needs of the industry.
- The industry group should be led by a suitable industry sponsor/champion.
- A study is undertaken by the industry sponsor/champion to identify and communicate the benefits of a reliability database to the industry and determine how commitment to this scheme by the members can be assured. This will also require actions to address issues with developers/suppliers about commercially sensitive/IP information being shared. Investigation of the OREDA model could assist with these issues.
- For a database to work effectively, processes, based on current industry best practices should be adopted to include;
  - A standard definition of Reliability across the industry.
  - A Common Tidal Turbine Taxonomy across the industry.
  - A clear definition of architectures that are applicable to the database.
  - An agreed data set to accompany all records entered into the database. (This could be based on an existing related system such as Reliawind for potential cross referencing on common parts)

A common robust and consistent “Root cause analysis” process is developed and used across the industry. FRACAS could provide this.

Note: The adoption of a process such as FRACAS together with an agreed industry wide Taxonomy will greatly assist in the establishment of a Tidal Turbine Reliability Database.

4.2 Physics of Failure

4.2.1 Objective

This phase of the DfR process is concerned with investigation of the Physics of Failure associated with critical components, in the absence of sufficient statistical data (i.e. Database material), due to small populations and varied load cases, and to make recommendations for:

- Improved accuracy of models for use at the Design phase by considering all loadings (external & internal).
- The opportunities to enhance Condition Based Monitoring from a Diagnostic based to a Prognostic based tool and ensure it is applied in the most effective manner to Tidal Turbines.

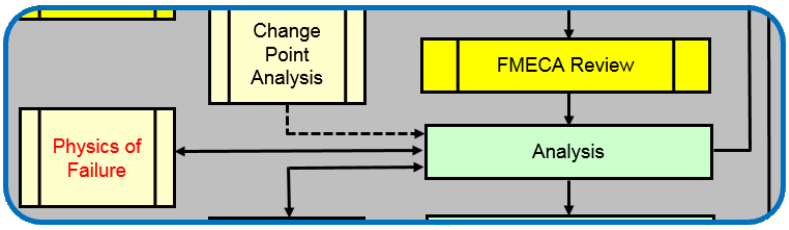

Figure 15 - Example of Physics of Failure process used within the Design Process (Design Iteration)

Report **RD.15/141601.1** - *Physics of Failure & Condition Monitoring Processes* considers the processes to address and understand failure mechanisms at their local level through Physics of Failure (PoF) techniques, and achieve a better understanding of specific failure mechanisms in use within Tidal Turbines.

Failure modes are considered and the traditional “bath tub” curve is expanded to more accurately reflect the real nature of failures, useful life and wear out, based on recent research.

As Wind Turbines (WT) represent, in their physical configuration, close analogies to Tidal Turbines, a review of available sensors is included in the above report based largely on those employed in WT’s. Additionally, as the focus of this report is Physics of Failure and associated sensors, the sensors considered are those which operate at sub-system level. These allow the acquisition of information on specific components and thus in the locality of potential failures.

Subsystem Condition Monitoring (CM) can be classified into two main subcategories: namely those based on Destructive Test (DT) and those based on non-destructive test (NDT). Both are discussed.

Note: The assumption is that components are made and assembled to specification. Beware of chasing failure mechanisms related to design when the fault lies with quality.

Note: It makes sense to have transferable data from FAT or factory in-process testing to inform CM strategies.

Note: Traceability and recording of relevant information and waveforms is essential.

Note: The "intensity" of effort for some of these types of investigations may make it more suitable to be undertaken by a supplier or University, specialising in this type of work.

4.2.2 Activities

The basic steps to implementing the PoF approach are the following:

- Defining realistic component / product requirements
- Defining the design duty cycle
- Define loads, load types (e.g. deterministic / stochastic) and characteristics
- The duty cycle will define the mechanical, thermal, electrical and chemical loads that are experienced over time. These loads may be associated with manufacture, testing, storage, repair, handling as well as operating conditions.
- Identifying potential failure sites and failure mechanisms. Critical parts and their interconnections, potential failure mechanisms and modes must be identified early in the design. Potential architectural and stress interactions must also be defined.
- Characterising the materials, manufacturing and assembly processes. It is unrealistic to assume materials are free of defects as they often have naturally occurring defects and manufacturing processes can also induce additional defects.
- Designing to the duty cycle and process capability. The design stress spectra and the full scale test spectra must be based on the anticipated life-cycle usage conditions. These steps become an iterative process of the system design, design analysis and system modification (re-design) See Figure 16, to develop a reliable, cost effective product that meets a set of realistic expectations.

The process of PoF analysis is unique for each component and its associated design, manufacture, duty cycle and environment and can be complex. To understand the mechanisms of failure as discussed above such as fatigue, fracture, thermal load, wear, and corrosion of components within systems, modelling and simulation (M&S) is used.

System-level, multi-body dynamics models can be created to accurately represent the operating platform (or sub-system) and determine resultant loads and accelerations at areas of interest due to induced loads (e.g., system shock load inputs).

System testing can be used to calibrate and validate the dynamics model as well as provide information to finite-element, static strength, buckling, and/or fatigue models.

Finite-Element Method (FEM) can be used to determine resultant stresses and strains based on predicted or test-measured loads. With this information, static strength analyses can be performed to determine if for example a single applied load is sufficient to cause failure (brittle or ductile fracture), buckling analyses can be performed to determine whether compressive loads are high enough to produce elastic instability, and fatigue analyses can be performed to determine time-to-failure based on repeated loads.

The above summary is not exhaustive but simply illustrates some of the techniques which can be used to determine loading at the material and environmental levels with suitable models.

The overall process of defining and analysing the system is illustrated in Figure 16

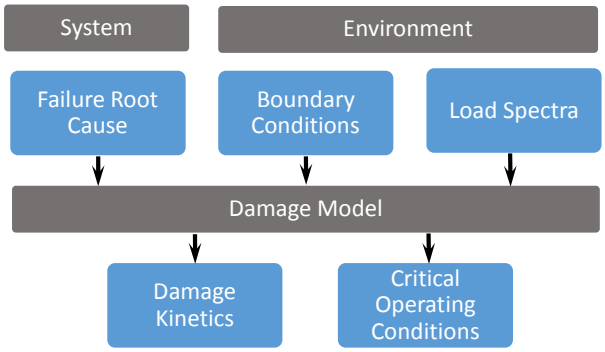

Figure 16 - Defining & Analysing the System for PoF

4.2.3 Deliverables

For each combination of failure mode and component, a damage model is used to calculate the rate at which damage accumulates in response to the operating environment. The model should represent a physically accurate description of the damage kinetics and should correctly identify critical operating conditions. Typically only those parameters that are known to have a significant influence on the damage kinetics should be considered in order to keep the model and sensor complexity as simple as possible, whilst achieving reasonable accuracy.

Note: PoF investigations will be enhanced by the "intelligent" use of advanced sensors, specific to the area being studied.

Ideally it should be possible to directly measure the parameters that are required as input to the damage model. In cases where direct measurement is not possible due to sensor limitations, then the damage model should also include some transfer function between the parameter that may be measured directly and that which is finally required for the definition of the damage kinetics. Such a transfer function may be based on classical analytical theory, experimental parameter mapping or simulation techniques such as the Finite Element Method (FEM) and Computational Fluid Dynamics (CFD).

The development of highly effective damage models should generally be viewed as a long term, iterative process. Typically, an initial model is proposed based on understanding of the problem physics and including an element of engineering judgement to identify the most significant influencing factors for a typical operating environment. Wherever possible this model is then validated by comparing the calculated damage kinetics with the results of experimentation and ideally with real life failure cases to confirm that critical operating conditions are correctly predicted. In some cases, such validation activities will reveal the need for improvements to the model such as the consideration of additional parameters or the inclusion of correction factors, possibly leading to a semi-empirical solution. This in turn may require the justifiable use of additional sensors but this approach should avoid sensor "overkill" from the start of the project.

To summarise, in the absence of reliability data for the component, these relationships can be used to predict with some confidence the Mean Time To Failure (MTTF) for a non-serviceable device such as a Tidal Turbine.

4.2.4 Process Intensity

The amount of input required to produce a Physics of Failure approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 17 below;

Figure 17 - Physics of Failure Process Intensity

4.2.5 Physics of Failure Checklist

- ✓ Have realistic component/product requirements been defined?
- ✓ Has the Duty Cycle been defined?
- ✓ Have all potential loadings been considered (mechanical, thermal, electrical and chemical)?
- ✓ Have loadings associated with manufacture, testing, storage, repair, handling as well as operating conditions been considered?
- ✓ Have potential "failure sites" and "failure mechanisms" been identified for models
- ✓ Is design stress spectra and full scale test spectra based on the anticipated life-cycle usage conditions?
- ✓ Have suitable models been developed
- ✓ Have suitable sensor types been identified for operating at failure sites.

4.2.6 Further Reading

RD.15/141601.1 : Physics of Failure & Condition Monitoring Processes

5 'Quantify & Improve'

5.1 Life Data Analysis

5.1.1 Objective

Life Data Analysis involves the prediction of lifetimes of products in a population using a representative sample drawn from the population. By fitting a statistical distribution to such a sample, an attempt can be made to estimate key life characteristics of Tidal Turbines, such as:

- Average/expected lifespan
- Failure rate as a function of the passage of time
- Reliability, or probability of failure at a particular point in time

Depending on the type of unit under consideration (component or sub-system), lifetime may be measured in terms of time, distance or cycles.

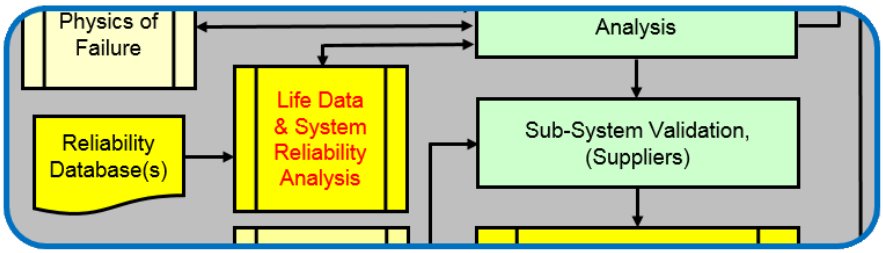

Figure 18 - Example of Life Data & System Reliability Analysis within the Design Process (Design Iteration)

Determining the reliability of manufactured systems such as Tidal Turbine devices often requires performing a life test at component, sub-system or system level and analysing observed times to failure. Such data (times to failure or other observed values) is frequently unknown or partially known. This is described as censored data, in that some items being tested may not have failed when the test is ended or they failed prior to an inspection but the exact time of failure cannot be determined. In addition, it may be necessary to accelerate failure times by changing the value of an influential variable (e.g. temperature). For all of these reasons, special processes are employed and can be generally described as Life Data Analysis.

If sufficient data is available, it may be possible to fit a specific distribution to the failure times. Once a suitable life distribution has been established and the confidence in the validity of the data is high, it is possible to calculate a large amount of useful data relating to the performance and reliability of the system.

5.1.2 Activities

Life data analysis requires the practitioner to:

- Gather life data for the product (component, sub-system, or system)
- Select a lifetime distribution that will fit the data and model the life of the product.
- Estimate the parameters that will fit the distribution to the data.
- Generate plots and results that estimate the life characteristics of the product, such as the reliability or mean life.

5.1.3 Deliverables

When the parameters to fit a life distribution to a particular data set have been calculated, a variety of plots and calculated results from the analysis can be obtained, including:

- Reliability Given Time: The probability that a unit will operate successfully at a particular point in time. For example, there is an 88% chance that the product will operate successfully after 3 years of operation.
- Probability of Failure Given Time: The probability that a unit will be failed at a particular point in time. Probability of failure is also known as "unreliability" and it is the reciprocal of the reliability. For example, there is a 12% chance that the unit will be failed after 3 years of operation (probability of failure or unreliability) and an 88% chance that it will operate successfully (reliability).
- Mean Life: The average time that the units in the population are expected to operate before failure. This metric is often referred to as "mean time to failure" (MTTF) or "mean time before failure" (MTBF).
- Failure Rate: The number of failures per unit time that can be expected to occur for the product.
- Warranty Time: The estimated time when the reliability will be equal to a specified goal. For example, the estimated time of operation is 4 years for a reliability of 90%.
- B(X) Life: The estimated time when the probability of failure will reach a specified point (X%). For example, if 10% of the products are expected to fail by 4 years of operation, then the B(10) life is 4 years. (Note that this is equivalent to a warranty time of 4 years for a 90% reliability.)
- Probability Plot: A plot of the probability of failure over time. (Note that probability plots are based on the linearization of a specific distribution. Consequently, the form of a probability plot for one distribution will be different than the form for another. For example, an exponential distribution probability plot has different axes than those of a normal distribution probability plot.)
- Reliability vs. Time Plot: A plot of the reliability over time.

- pdf Plot: A plot of the probability density function (pdf).
- Failure Rate vs. Time Plot: A plot of the failure rate over time.
- Contour Plot: A graphical representation of the possible solutions to the likelihood ratio equation. This is employed to make comparisons between two different data sets.

5.1.4 Process Intensity

The amount of input required to produce a Physics of Failure approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 19 below;

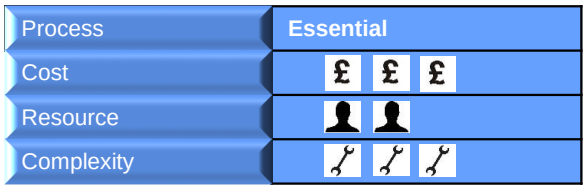

Figure 19 - Life Data Analysis Process Intensity

5.1.5 Life Data Analysis Checklist

✓ Is there a sufficient quantity of data to undertake Life Data Analysis?

✓ Has “censored” data been considered in the analysis?

✓ Has a suitable life distribution has been established (with confidence)?

✓ Does any later data still fit the model?

✓ Have all the “life characteristics” of the product model been calculated?

5.1.6 Further Reading

RD.15/001038.1 – Life Data Analysis & System Reliability Analysis

5.2 System Reliability Analysis

5.2.1 Objective

In System Reliability Analysis a "System" model is constructed from the component models previously analysed. In other words System Reliability Analysis is concerned with the construction of a model (life distribution) that represents the times-to-failure of the entire system based on the life distributions of the components, subassemblies and/or assemblies ("black boxes") from which it is composed.

A system is a collection of components, subsystems and/or assemblies arranged to a specific design in order to achieve desired functions with acceptable performance and reliability. The

types of components, their quantities, their qualities and the manner in which they are arranged within the system have a direct effect on the system's reliability. To accomplish this, and in addition to the reliability of the components, the relationship between these components is also considered and decisions as to the choice of components can be made to improve or optimize the overall system reliability, maintainability and/or availability. This reliability relationship is usually expressed using logic diagrams, such as;

- Reliability Block Diagrams (RBD) and/or
- Fault Trees

5.2.2 Activities

The key to reliability analysis at a system level is the ability to describe the relationship between components in a system in a mathematical format.

Operating within the RBD framework, the relationships between components are considered and decisions about the choice of components can be made to improve or optimise the overall system reliability, maintainability and/or availability. There are many specific reasons to look at component data to estimate the overall reliability of a system or sub-system to which it belongs. One of the principal reasons is that for devices such as Tidal Turbines, it is easier and less expensive to test component / sub-systems rather than entire systems.

5.2.3 Deliverables

The importance of System Reliability Analysis as a tool lies with establishing the influence of Components-off-the-Shelf (COTS), within a Tidal Turbine System. While much analytical work may be carried out on bespoke components or systems, COTS are often overlooked in terms of their effect on system reliability. The selection of an off-the-shelf component is often based solely on lowest cost which is often accompanied by a lack of information or knowledge by the supplier on the reliability of the part supplied. The adoption of System Reliability Analysis disciplines and the use of RBD’s within the DfR tools will drive an increased awareness with the Tidal Turbine developer and contractual requirements on the component supplier, for reliability data to underpin the selection and use of appropriate COTS to meet the reliability target of the system.

5.2.4 Process Intensity

The amount of input required to produce a System Reliability Analysis in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 20 below;

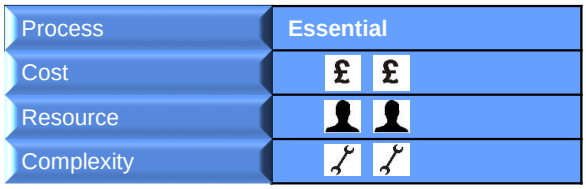

Figure 20 - System Reliability Analysis Process Intensity

5.2.5 System Reliability Analysis Checklist

- Have Reliability Block Diagrams or fault trees been completed and do they describe the correct algebraic relationships between components or sub-systems?
- Is all “actual” reliability data available?
- Are suitable “reliability estimates” available where required?

5.2.6 Further Reading

RD.15/001038.1 – Life Data Analysis & System Reliability Analysis

5.3 Design of Experiments

5.3.1 Objective

Design of experiments (DoE) is a systematic method to determine the relationship between factors affecting a process and the output of that process. It is used to find cause-and-effect relationships. The term “process” can be applied to the function of a component, sub-assembly or assembly when referring to the conversion of the known input to the desired output as illustrated in Figure 21. This information is needed to manage process inputs in order to optimize the output.

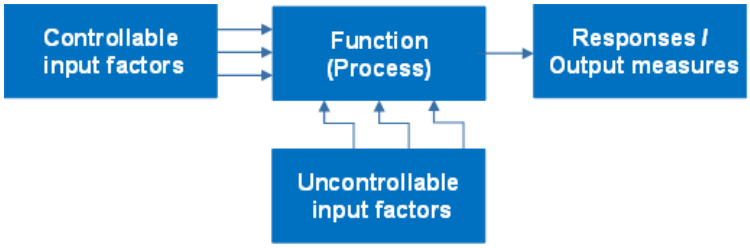

Figure 21 - Process Factors & Responses

- The objective of DoE as a tool in reliability engineering and quality is to investigate key interactions which, when identified, can be used at various stages to improve both quality and reliability as part of the Design for Reliability methodology for Tidal Turbines. Examples of the use of this technique can include the following design & development process stages:
- Design optimisation
- Process optimisation

- Supplier selection
- Root Cause Analysis
- “What-If” Analysis
- Component & Sub-System testing
- Noise factor optimisation & management.

Note: DoE should be used anywhere in the DfR process where data on “Effects” or “Interactions” are required.

In general, it can be used at many stages of the Design for Reliability process when more than one input factor is suspected of influencing an output and the influences require understanding and quantifying.

5.3.2 Activities

Running DoE projects requires a detailed knowledge of some statistical tools and training in the various techniques employed. The scope of this summary report does not cover any detailed DoE techniques but more details (including a worked example) can be found in report **RD.15/001027-1**: *Design of Experiments*, which includes references to other works dealing with DoE processes.

In order to undertake a DoE, certain conditions must be known and understood. The steps below describe the process in outline only:

- A full understanding of the inputs and outputs being investigated is required. A process flow diagram or process map can be helpful. The use of subject matter experts can be useful for complex processes.
- Determine the appropriate measure for the output. A variable measure is preferable. Attribute measures (pass/fail) should be avoided as they do not represent actual values (variables). Ensure the measurement system is stable and repeatable.
- A design matrix should be created for the factors being investigated. The design matrix will show all possible combinations of high and low levels for each input factor. These high and low levels can be generically coded as +1 and -1. For example, a 2 factor experiment will require 4 experimental runs:
- For each input, the extreme (but realistic) high and low levels to be investigated should be determined. In some cases the extreme levels may be beyond what is currently in use. However, any extreme levels selected should be realistic.

- Enter the factors and levels for the experiment into the design matrix. Perform each experiment and record the results.
- Calculate the effect of a factor by averaging the data collected at the low level and subtracting it from the average of the data collected at the high level.
- Plot the Main Effects to allow visual comparison of the relative size of the effects. This is done by plotting the “+1” and “-1” average values for all the Factors and joining with a line. An example of such a plot is shown in Figure 22. It should be noted that the mid-points of all the lines is the same. This midpoint is known as the “Grand Average”.

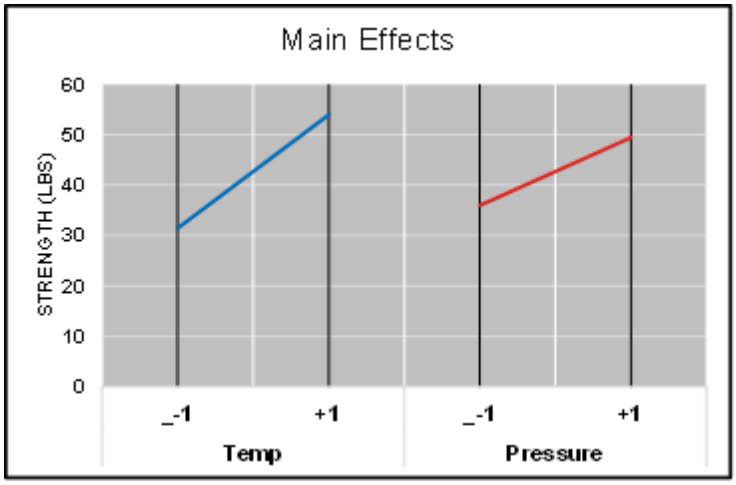

Figure 22 - Example of a Main Effects Plot (Example shows Temperature & Pressure)

Note: For complex multi-factorial experiments it is important that the correct skills are available to run the experiment.

5.3.3 Deliverables

When two things occur which produce a magnified result, this is described as an Interaction. Interactions can work against the system being investigated and can indicate areas to be addressed. However, interactions can also work for the system when the magnified response is the desired output. Performing a full factorial experiment allows calculation of interactions without any further experimental work. Referring to Figure 22 above, where lines are not parallel (in their gradient) this can indicate an interaction between the factors is present

The interaction between two factors can also be calculated in the same way as the Main Effects above. First, the design matrix must be amended to show the high and low levels of the interaction. The levels are calculated by multiplying the coded levels for the input factors acting in the interaction.

5.3.4 Process Intensity

The amount of input required to produce a Design of Experiments approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 23 below;

Figure 23 - Design of Experiments Process Intensity

5.3.5 Checklist

- ✓ Has the need for an “experiment” been demonstrated?
- ✓ Are the correct Inputs and Outputs known and understood?
- ✓ Have appropriate “variables” been chosen for the measurables?
- ✓ Has a design matrix been created with the appropriate factors?
- ✓ Have acceptable “extremes” been chosen for the “variables”?

5.3.6 Further Reading

RD.15/001027-1 – Design of Experiments

5.4 Fault Tree Analysis

5.4.1 Objective

Fault Tree Analysis (FTA) is a top-down, logical process for acquiring information about a system. This information is then used for identifying potential causes of failures.

When used at the design stage of a project, an FTA can help with mitigating against possible failures by ensuring that the design team considers failure modes and includes appropriate risk reduction measures in the design. While this sounds similar to the Failure Modes and Effects Analysis (FMEA) process, an FTA considers the relationships between parts, rather than being single function focused.

As a fault finding tool, FTA provides a logical representation of the elements in a system. The process of constructing a fault tree allows the investigating team to consider the relationships between the parts at each level of the system. On a subjective level, this can help with

uncovering potential failure causes. FTA can also be used to study probability of failure by mathematically evaluating the relationships using Boolean algebra.

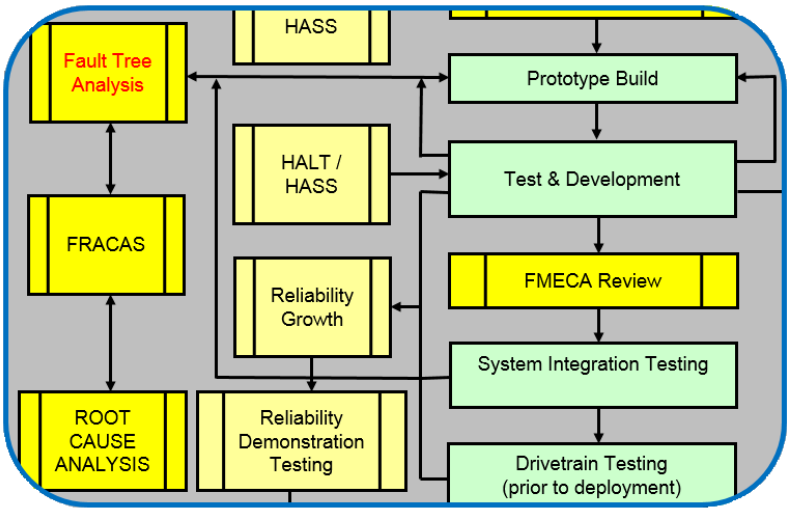

Figure 24 - Example of Fault Tree Analysis within the Design Process

Note: One of the strengths of FTA is that it can identify multi-point failures.

FMEA's and FMECA's only identify single point failures!

5.4.2 Activities

5.4.2.1 Defining the Problem and Setting Boundaries

It is important for the success of the analysis that the top level failure event is carefully defined. If the definition is too general, the analysis will develop into a very large fault tree, and thus become unwieldy, and perhaps confusing.

If the fault definition is too specific, the analysis will probably not examine the system to a wide enough level, and might miss potential causes of the fault.

The scope of the fault definition can be bounded by considering what aspect of system performance is of concern. For example, in the case of a gear failure in a tidal turbine gearbox, the fault definition could be "gearbox fails to provide input torque to generator". This fault definition would limit the fault tree to the gearbox, generator and parts relating to these.

It is also necessary to set a limit of resolution. This is the level of detail to which the investigation should extend when considering component parts. For example, should an investigation into a gearbox delve right down to the level of component parts in a bearing – ball

bearings, races, shields, etc.? Probably not, as these will be the responsibility of the bearing supplier.

5.4.2.2 Constructing the Fault Tree

The fault tree is constructed using the following logic steps as the basis:

- An undesired event is defined
- The event is resolved into its immediate causes
- This resolution of events continues until basic causes are identified
- A logical diagram called a fault tree is constructed showing the logical event relationships

The fault tree is the logical model of the relationship of the undesired event to more basic events.

Within the fault tree, the top event is the undesired event.

The middle events are intermediate events.

At the bottom of the tree are the causal basic events or primary events. These are the component failures that lead to the undesired, or top, event occurring.

A simple fault tree for a basic electric motor circuit is shown below in Figure 25, to illustrate the various levels of events.

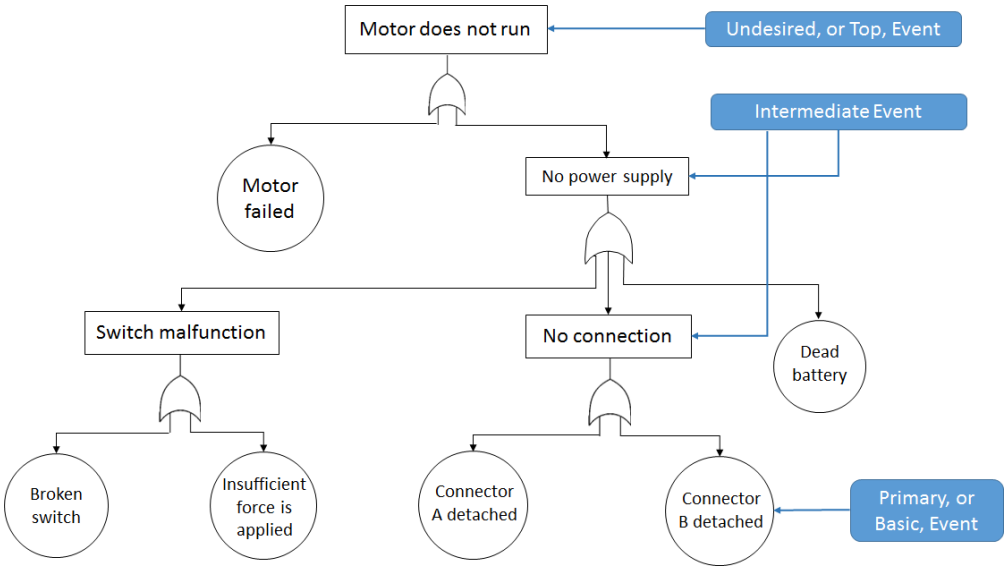

Figure 25 - Simple Fault Tree showing event types

5.4.2.3 Collecting the minimal cut or route set

Once the fault tree has been constructed, analysis of the possible causes can begin. In many cases, the analysis is done using Boolean equations for the possible causes identified. This allows both qualitative and quantitative evaluation of the fault tree to be performed.

A "minimal cut set" can be defined as the smallest combination of component failures which, if they all occur, will cause the top event to occur

5.4.3 Deliverables

By using the fault tree at a more subjective level, it should be possible to identify the more likely causes, or component failures, which lead to a system fault, based on the engineering judgement and experience of the team evaluating the fault tree. The use of basic descriptive terms in the immediate cause boxes should make the fault tree more accessible in terms of understanding possible failure causes.

If reliability data is available for the component parts of a system, this can be used in the developed Boolean equations, and probability of certain component and sub-system failures developing can be estimated.

Developing a fault tree while at the design phase of a project, allows identification of the parts, and combinations of parts, that should be examined in the FMEA. The FTA can also help to identify the potential failure modes to be considered during the FMEA process.

As an example of the fault tree usage at the design stage, a design specification might state that no single component failure shall lead to a system failure. This is the same as saying that the system should contain no single component minimal cut sets. Thus, checking the minimal cut sets can confirm that this design requirement is met. Similarly, if the specification states that a certain type of failure should not fail the system, the fault tree can be used to verify that this is being met.

5.4.4 Process Intensity

The amount of input required to produce a Fault Tree Analysis in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 26 below;

Figure 26 - Fault Tree Analysis Process Intensity

5.4.5 Fault Tree Analysis Checklist

- ✓ Has problem been correctly defined?
- ✓ Has top level failure event been correctly defined?
- ✓ Has the scope of the fault definition been bounded by considering what aspect of system performance is of concern?
- ✓ Has the limit of resolution been defined? This is the level of detail to which the investigation will extend when considering component parts?
- ✓ Have “AND” & “OR” gates been correctly defined throughout the system?
- ✓ Have any “conditional” causes been identified and applied to the model?

5.4.6 Further Reading

RD.15/001035-1 – Fault Tree Analysis

5.5 Reliability Growth

5.5.1 Objective

Reliability Growth (RG) is defined as the positive improvement in a reliability metric of a product (component, sub-system, system) over a period of time due to changes in the products design and / or manufacturing process. An RG programme is a structured process of finding reliability problems by testing, incorporating corrective actions and monitoring the increase of the products reliability throughout the test phases. The term “growth” is used since it is assumed that the reliability of the product will increase over time as design changes and fixes are implemented. However, in practice it is possible in some cases that no growth or negative growth may occur.

Reliability Growth is considered an essential process within the Tidal Turbine Design for Reliability methodology. This activity will be foremost in demonstrating and providing data to confirm the improvements achieved throughout the complete DfR process.

The fundamental concept of Reliability Growth is that the reliability of an item will improve as failure modes that degrade its function are discovered and eliminated or mitigated.

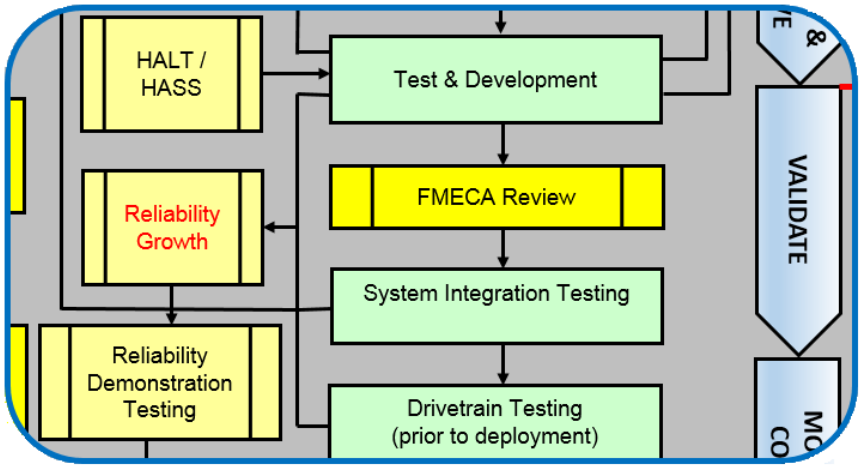

Figure 27 - Reliability Growth within the Test Phases of the Design Process

Some systematic failure modes may be revealed early in development whereas others may take considerable time to be revealed. Some will be easily diagnosed and solutions implemented but the cause of others may be difficult to identify, diagnose and remedy. Throughout the life of the item therefore, there will generally be latent failure modes waiting to be discovered and corrected by design or other changes.

5.5.2 Activities

The rate at which reliability will "grow" towards the specified target will depend upon the rate at which:

- Failure modes are detected
- Failure information is made available to the responsible design / development authority and failure causes investigated.
- Re-design or other changes are made to overcome the reported failures.
- The modifications are introduced and checked to ensure that they are effective.

To ensure that reliability reaches a specified target within a given time, methods are required which will assess the progress in growth and hence guide management in controlling the activities that influence it.

The concept of RG management only applies during the development phase when a controlled testing programme is used. It is only under these conditions that practical relationships can be established between the growth process and the resources that stimulate growth.

To achieve significant growth during development, the reliability test programme must be thoroughly planned and funded from the outset. The planned values of reliability to be expected at any stage of the test programme must be determined and estimates made of the time, resources and funding required to achieve these planned aims.

Mathematical growth models provide the main method for quantifying a growth programme so that it can be effectively planned, monitored and controlled. Various growth models have been developed to represent the RG process during development and these are discussed in greater detail in documents such as Def Standard 00-42 Part 2, MIL-HDBK-189C, IEC 61508 and BS 5760.

Examples of models that can be used include:

- Duane
- AMSAA – Crow Planning Model
- Subsystem Level Planning Model (SSPLAN)
- Generally, the selection of a growth model for a particular project application will depend largely on previous experience. The main requirements are:
- The model must be practical even at the expense of some accuracy. For example consideration must be given to ease of parameter estimation, flexibility to adapt to varying growth situations, ease of computation, etc.
- The model must be valid for the intended application.
- The model must provide clear management information on which progress can be judged and actions/decisions taken.

For further information on the detailed techniques for Reliability Growth management, monitoring and control, refer to Report **RD.15/001048.1** - *Reliability Growth and Reliability Demonstration Testing* and additionally, the included Bibliography referenced within the report.

5.5.3 Deliverables

Figure 28 shows an example of a typical RG curve across the development test phases of a programme. This illustrates the effect of the Test-Fix-Test approach to the introduction of reliability improvements and is a preferred approach provided changes can be implemented quickly. The curve shown is continuous but in reality, there is a time lapse between phases which will allow for the introduction of revised parts for the next test phase.

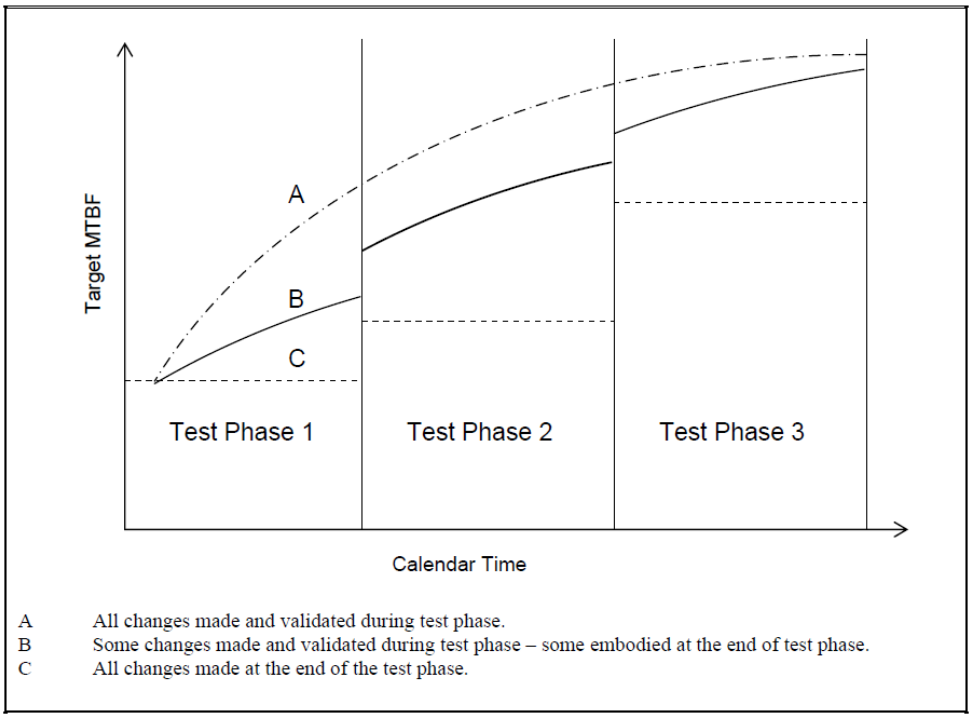

Figure 28 - Sample Reliability Growth Curve for a Test Fix Test programme

Replacing a part with an identical part will not increase reliability. An enhancement has to be made to the function of the part to do this.

Fixing a part could actually reduce reliability if it "unmasks" another failure hidden or protected by the original part.

5.5.4 Process Intensity

The amount of input required to produce a Reliability Growth approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 29 below;

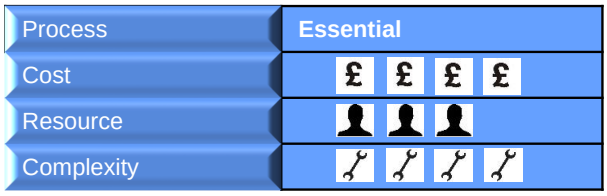

Figure 29 - Reliability Growth Process Intensity

5.5.5 Reliability Growth Checklist

✓ Has a Reliability Growth (RG) plan been created at the start of the programme?

✓ Has a suitable budget been approved for RG?

- ✓ Has a Reliability Target been established?
- ✓ Have all prototype phases been defined?
- ✓ Has a suitable RG model been selected for the programme?
- ✓ Has the strategy for “fixes” been agreed (e.g. Test, Fix, Test etc.)?
- ✓ Have suitable skills been employed for RG tracking.

5.5.6 Further Reading

- **RD.15/001048.1** - Reliability Growth and Reliability Demonstration Testing
- US Department of Defense, “Handbook for Reliability Test Methods, Plans and Environments for Engineering Development Qualification and Production.” **MIL-HDBK-781A**, 1 April 1996
- MoD. “Applied R&M Manual for Defence Systems – Chapter 40 Reliability Demonstration - Part C - Techniques”, Mod, May 2012

5.6 HALT/HASS/ALT

5.6.1 Objective

In HALT and HASS testing, stresses are applied in a controlled, incremental fashion while the unit under test is continuously monitored for failures. Once the weaknesses of the product are uncovered and corrective actions taken, the limits of the product are clearly understood and the operating margins have been extended as far as possible. The result is a more mature product (component, sub-system) which can be introduced with a higher level of confidence in its reliability within a system than products which have undergone less rigorous investigation at the development stages.

Accelerated Life Testing (ALT) is used where qualitative life data is required or the testing of parameters such as wear-out is required. These cannot be achieved using the HALT process.

Accelerated Life Testing (ALT) which should not be confused with HALT & HASS tests, is carried out with pre-determined (calculated) stress models and accelerators with the objective of observing only one failure mechanism per test. All other failure modes will result in “censored run times”.

Life data for a part cannot be extrapolated from a HALT test. This can only be done in an ALT.

5.6.2 Activities

5.6.2.1 HALT Testing

Unlike DVT (Design Verification Testing), the purpose of HALT is to determine the operating and destruct limits of a design - why the limitations exist and what actions will be required to increase those margins. HALT, therefore, stresses products beyond their design specifications. See Figure 30 below

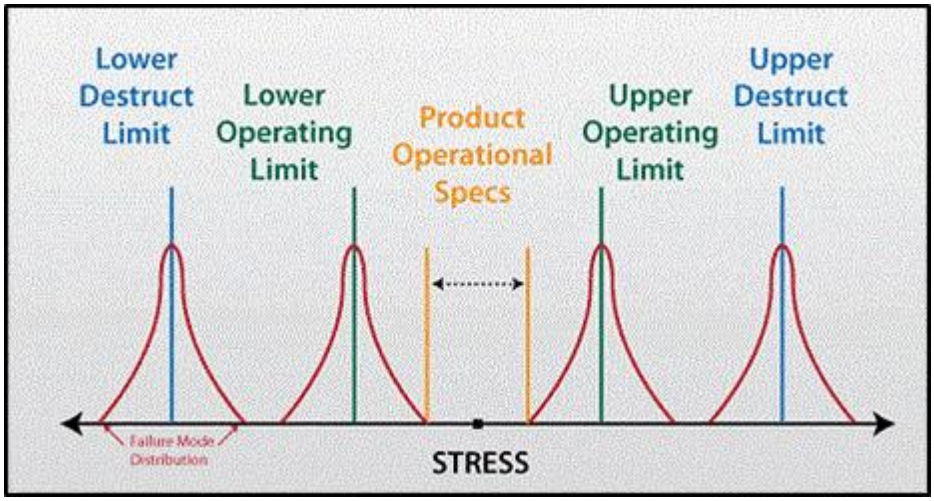

Figure 30 - The scope of HALT tests extends to 'Destruct Limits'

During the HALT process, a component/sub-system is subject to increasing stress levels of temperature and vibration (independently and in combination), rapid thermal transitions, and other stresses specifically related to the operation of the product.

The information goals of HALT are to:

- Determine multiple failure modes and root causes
- Determine functional operating limits
- Determine functional destruct limits
- Focus on thermal and vibration stresses (first separately, then combined)

5.6.2.2 HASS Testing

In a HASS test, a component, or several are pulled from production and subjected to a series of tests that simulate the highest possible stresses that the component will see, possibly exceeding the operational limits of the product specification. Using the concept of time compression, these tests show in a short time that the component is operating correctly, that it has an acceptable level of robustness and that there are no errors being introduced through the manufacturing process. This (in addition to normal quality processes) also provides some safeguards against excessive manufacturing process “drift” or material defects etc. This “in-

process” batch testing ensures that the process is continuously intact and that the component meets and exceeds specifications.

5.6.2.3 ALT Testing

Accelerated Life Testing (ALT) is a combination of statistics, engineering and physics of failure. Stress is increased during the test in order to excite the mechanism of failure and cause it to occur in a shorter period of time relative to the field operation. The underlying physics of failure need to be understood prior to performing the test; otherwise, the test could simply be of no value. A successful accelerated life test requires:

- A good understanding of the failure mechanisms to be accelerated.
- A good understanding of the factors affecting the failure mechanisms.
- A determination of the intensity levels of these factors.

The above elements can be attained by investigating the underlying physics governing the mechanisms of failure or from engineering experience. The factors that determine a product's life behaviour, such as the material, geometry and technology, can be correlated to the above mentioned elements, thus resulting in a well-executed ACT. For instance, given the material of the product, it can be known that exceeding a certain stress level will result in unrealistic failures (i.e., failure modes that would not occur under normal use conditions). These levels, if unknown, can be established using HALT techniques in advance.

Even if all of the first three elements are considered, it needs to be ensured that the accelerated test will yield failures within the allowable test time. So the fourth element in the list is:

- Sufficient test time.

5.6.3 Deliverables

HALT/HASS tests offer preliminary techniques to evaluate the upper and lower limits of loading (thermal, electrical, stress, strain, temperatures, voltage, vibration rate, pressure etc.) close to the “destruct” limits of the design. Preliminary improvements based on this data alone will contribute towards earlier design maturity.

ALT is a more structured process where life distributions are considered for the parameter being ”accelerated” which will provide the means to extrapolate results back to expected performance under normal duty cycles. ALT can use the results of a HALT test to evaluate maximum expected loadings (stress, strain, vibration temperature etc.)

5.6.4 Process Intensity

The amount of input required to produce a HALT/HASS/ALT approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 31 below

Figure 31 - HALT/HASS/ALT Process Intensity

5.6.5 HALT/HASS/ALT Checklist

- ✓ Is the components application suitable for HALT or ALT tests?
- ✓ Have the operating limits been estimated (if not defined)?
- ✓ Have changes as a result of HALT testing resulted in improvements on re-test?
- ✓ Do failure modes represent what might be expected in the field (discussion)?

5.6.6 Further Reading

RD.15/001168.1- Highly Accelerated Life Test (HALT), Highly Accelerated Stress Screen (HASS) & Accelerated Life Test (ALT)

6 'Validate'

6.1 Reliability Demonstration Testing

6.1.1 Objective

Reliability Demonstration Testing (RDT) should not be confused with Reliability Growth (RG) – See section 5.5, and its associated processes such as Test, Analyse, Fix (TAF) although in many respects these activities have aspects in common. RDT is mainly concerned with measuring whether or not a specified requirement has been met, normally in terms which can be contractually binding. It may itself reveal new failure modes which require corrective action, especially if there are inadequacies in the RG programme and associated tests. There is a relationship between RG and RDT and these activities should be planned with consideration to both processes.

The execution of Reliability Demonstration testing for Tidal Turbine devices will probably only be driven by a contractual requirement between the supplier and the customer. The exact conditions will depend on the nature of the contract, however, it is essential that reliability targets included in any contract are realistic, can be demonstrated practically and any outcomes are enforceable.

RDT should be considered by developers as a pre-delivery activity when the contract includes severe penalties for poor reliability performance. Here RDT can act as a project risk assessment tool.

6.1.2 Activities

The specification, planning and execution of a successful RDT programme, will require a team, suitably qualified in reliability processes and a thorough understanding of the associated statistical techniques in order to process and correctly interpret the data outputs. This must be underpinned by a commitment from management and an adequate budget to implement what will be one of the most expensive and complex activities within any DfR methodology.

The detailed processes to be followed are beyond the scope of this summary report but the Principals of Demonstration, Requirements, Planning, and Implementing are extensively detailed in various publications, some of which are listed in the References and Bibliography of Report **RD.15/001048.1**: *Reliability Growth and Reliability Demonstration Testing*.

6.1.3 Deliverables

An RDT demonstrates whether the achievement of given reliability parameter values can be claimed with a given level of confidence. This definition is deliberately couched in terms of "claimed" and "confidence" since statistical parameters are being addressed and the

parameters cannot be measured exactly and repeatedly in tests based on small samples. For example if a system is tested for 500 hrs and exhibits 5 failures it can be claimed (assuming a constant failure rate) that:

a. The MTBF is at least 50 hrs with a confidence of 0.93:

b. The MTBF is at least 100 hrs with a confidence of 0.38: and

c. The MTBF is at least 150 hrs with a confidence of 0.04.

All of these statements are correct from the results quoted. Note that the higher the claim, the lower the level of confidence.

6.1.4 Process Intensity

The amount of input required to produce a Reliability Demonstration Testing approach in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 32 below

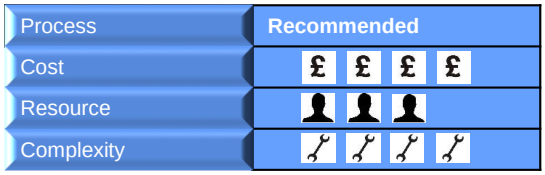

Figure 32 - Reliability Demonstration Testing Process Intensity

6.1.5 Reliability Demonstration Testing Checklist

✓ Have the reliability requirements been defined at the start of the programme?

✓ Has “reliability” been defined in a way it can be demonstrated?

✓ Does RDT form part of a supplier contract?

✓ Has RDT been budgeted (cost & resources) within the programme?

6.1.6 Further Reading

RD.15/001048.1 - Reliability Growth and Reliability Demonstration Testing

7 'Monitor & Control'

7.1 Root Cause Analysis

7.1.1 Objective

As part of the understanding of failures and their causes, Root Cause Analysis (RCA) is a crucial element in the product development process. In the context of a Design for Reliability (DfR) process, RCA will be needed in support of a Failure Reporting, Analysis and Corrective Action System (FRACAS) – See section 7.2.

RCA will allow an organisation to:

- Find out what happened
- Find out why the failure happened
- Develop a plan to reduce the likelihood of it recurring

If not carried out in a structured way, RCA can lead to possible failure causes being overlooked, and the true cause of a failure potentially not being fully understood. This will ultimately have implications for the product development process, as failure causes will not be discovered, and failures will recur, either in later testing phases, leading to delays or more seriously, in production volume manufacturing by customers.

An effective root cause analysis process should meet the following criteria:

a) Clearly defines the problem and its significance to the problem owners.

b) Clearly delineates the known causal relationships that combined to cause the problem.

c) Clearly establishes causal relationships between the root cause(s) and the defined problem.

d) Clearly presents the evidence used to support the existence of identified causes.

e) Clearly explains how the solutions will prevent recurrence of the defined problem.

f) Clearly documents the above five criteria in a final RCA report so others can easily follow the logic of the analysis.

7.1.2 Activities

7.1.2.1 Define the problem

The problem has to be clearly understood before any resolution can be identified. This might be achieved by gathering data of operating conditions before, during and after the failure event.

7.1.2.2 Establish the team

The problem solving team should be comprised of personnel who can actively contribute to the process, bring skills such as data collection and analysis, varying functional backgrounds, (e.g. manufacturing, design, testing, service, etc.), specialist expertise, problem solving methodology and leadership skills, and someone who is prepared to ask the obvious questions that others might shy away from.

7.1.2.3 Contain the problem

Any containment action decided upon, should be validated to ensure that it does not have any negative effects on the original or adjacent parts or system (i.e. make the original problem worse). Note that containment, or emergency actions, are not intended as a substitute for full problem resolution. The root cause of the problem should be investigated and fully understood, and a solution developed.

7.1.2.4 Define root cause

The aim of this step is to identify all possible root causes that can produce the observed symptoms, and then using data, to identify and validate the cause of the actual problem.

Some of the processes used in root cause analysis are described in Report **RD15-000834-1** : *Root Cause Analysis Methodology*.

Always remember there can be more than one root cause for a failure.

7.1.2.5 Develop a permanent corrective action

The objective at this phase is to develop solutions that prevent the identified root causes recurring. Often the countermeasure can be identified intuitively once the root cause is known; however, there will also be cases where it might require a team effort to define the corrective action needed, and more detailed thought processes are required. Teamwork and brainstorming are often valuable at this phase.

The corrective action should be validated to ensure that it addresses the problem root cause, and that it does not introduce new failure modes to the part or system.

7.1.2.6 Implement permanent corrective action

The action(s) identified above are put into effect during this phase. The removal of containment actions and the introduction of permanent corrective actions should be planned and tracked carefully. The point of introduction (unit serial number, date, time, shift, etc.) should be recorded for reference in case of future failures with a new root cause or recurrence of the same problem.

Corrective actions should always be monitored beyond the life of the original failure.

It is important to monitor this stage closely to ensure that the original problem does not recur, or if it does, the cause is identified so that it does not lead to the original failure mode.

7.1.2.7 Monitor Effectiveness

This phase is to monitor the actions put in place at phase 7, to ensure that all the systems that support the corrective action are updated, and that any issues in the previous procedures which contributed to the failure have been addressed.

This will often mean updating design guidelines, service procedures, adding instrumentation, revising alarm settings, etc. It is important that there are checks in place to ensure the fix is working, and that any revised procedures are being observed.

7.1.3 Deliverables

The final output of a RCA process is a solution which has been proven to address the Root Cause and validated as a Permanent Corrective Action. Its implementation should not have any adverse effects on the surrounding system (unless, in solving a specific Root Cause, this has exposed another which was previously protected or masked by the original fault or failure)

7.1.4 Process Intensity

The amount of input required to produce a Root Cause Analysis in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 33 below

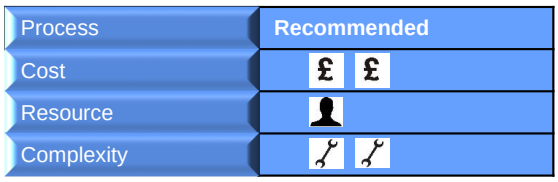

Figure 33 - Root Cause Analysis Process Intensity

7.1.5 Root Cause Analysis Checklist

- ✓ Has problem been correctly defined in terms of the customer?
- ✓ Is the correct team deployed?
- ✓ Has the problem been contained?
- ✓ Has the root cause(s) been defined and verified.
- ✓ Has the solution been implemented and is it effective?

✓ Does the solution cause any “new” failures or unmask any other existing failures?

7.1.6 Further Reading

RD15-000834-1: Root Cause Analysis Methodology

7.2 FRACAS

7.2.1 Objective

An essential part of the methodology for optimising reliability is the reporting of failures, their causes and the corrective actions taken to rectify the problem and reduce the probability of their future recurrence. When recorded in a suitable manner, this information can be used by both manufacturers and suppliers, to understand the weakness of a particular part or system; and to use the lessons learnt from the corrective actions in, for example, the design of new products, the specifying of maintenance schedules, and the effects of breakdowns on a system’s operational availability.

The Failure Reporting, Analysis and Corrective Action System (FRACAS) is a “closed loop” system used to improve the reliability of a product, service, process, or software application. The “closed loop” in FRACAS refers to the systematic manner in which every issue that is reported is addressed, ensuring that no failure or incident is missed.

7.2.2 Activities

7.2.2.1 Identifying the team

The FRACAS will require the involvement of a multi-disciplined team with members from across the organisation

7.2.2.2 The FRACAS process

The process detailed in this report is based on the overview given in section 8 of report number **RD.14/346801.1**, *Engineering Design for Reliability Processes Applicable to Tidal Turbines*. Figure 34 shows the FRACAS flowchart activities.

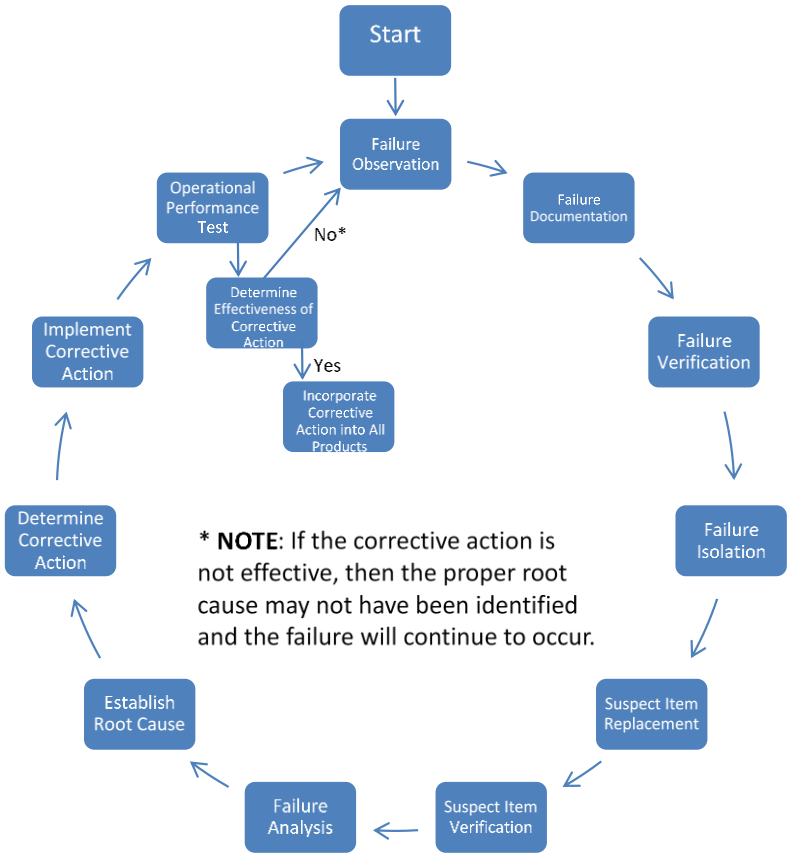

Figure 34 - FRACAS process flow diagram

7.2.2.3 Starting the process – Failure observation

For the development of the FRACAS process in this report, the definition of a failure is:

- An event in which an item does not perform one or more of its required functions within the specified limits under specified conditions.

A failure can be either catastrophic (total loss of function), or out-of-tolerance (degraded function beyond specified limits).

When an event such as this occurs, it should be the catalyst for the FRACAS process to begin.

7.2.2.4 Failure Documentation

The detailed documentation of a failure, and all the material, environmental and operating conditions around it, is key to an effective failure analysis.

It is important that a suitable failure reporting system is in place by the time testing begins. This will then facilitate the recording of any early-life failures that might be encountered, as well as those that arise later in the test programme. Those personnel involved with the inspection and testing of the equipment should be properly trained in how to complete the failure report forms with all the relevant details, preferably in an electronic format for database management.

7.2.2.5 Failure Verification

After a failure has been recorded, it must be verified before further actions can be taken. Verification can be achieved either by repeating the failure mode on the reported item (difficult in the context of an operational tidal turbine), or by actual evidence of the failure, such as damage to component(s), residue from a leakage, Built-in-Test indication, etc.

7.2.2.6 Failure Isolation

Isolating the failure is an extension of the failure verification process, by which the failed component or sub-system can be traced down to its lowest level.

7.2.2.7 Suspect Item Replacement

When replacing a suspect item, if possible, that item should be tested under similar conditions to those in which the original failure occurred. A failure under these conditions will verify that the identified item was in fact the cause of the failure. Note that this is not a substitute for failure root cause analysis.

The nature of tidal turbine operation is such that replicating exact under-sea operational conditions in a rig environment might not always be possible. For this reason, it might not be feasible to always include this step in the FRACAS process.

7.2.2.8 Failure Analysis

When the failure event information has been logged in the reporting system, the investigation into the failure root cause and the development of a corrective action can begin. By using FRACAS to record the details of the root cause analysis and its findings, a database of historical references will be built up and can be used to guide future failure investigations. Actual failure modes can be compared with those identified during the FMECA process, to determine if experienced failure modes are consistent with predicted failure modes.

7.2.2.9 Establish Root Cause

Each reported failure should be analysed to determine the root cause of failure. Analysis should consist of any relevant method and could include mechanical tests, material and chemical analysis, electrical tests, X-ray analysis, microscopic inspection, etc. as required to determine the failure cause.

7.2.2.10 Determine Corrective Actions

Corrective actions can include, but are not limited to, design changes, material changes, test procedure changes, and manufacturing method changes. The corrective action decided upon should be documented in the FRACAS, as part of the failure report. It is recommended that not only the type of action is recorded, but also the detail of the action or change, and the part or system to which it is applied.

7.2.2.11 Implement Corrective Action

Once a corrective action has been decided upon, a plan for its introduction should be made. When considering implementation of corrective actions it is important to remember that elimination of problems early in a programme is better, as the later corrective action is taken the more difficult and costly it can become. For this reason, it can be better to implement a corrective action as it becomes available, rather than waiting for a convenient programme milestone at which to introduce it.

7.2.2.12 Operational Performance Test

When a corrective action has been decided upon, it should be tested and monitored to ensure that the existing problem root cause is eliminated, and that the solution does not give rise to new problems in the system.

7.2.3 Deliverables

When the effectiveness of the corrective action has been verified, the timing for introduction into the next unit build, or build phase, can be planned.

The point of implementation should be recorded; e.g. the serial number of the first part or assembly in which the rectification is present, or for mass-produced parts, the date, time, and shift in which the change is first introduced. This will help with tracking corrective actions and verifying their effectiveness. It will also be useful if, in the case of future failures, the need to understand the maturity of a part is required.

7.2.4 Process Intensity

The amount of input required to produce a FRACAS in terms of cost, resource, and complexity, can be termed the process intensity, and can be graphically represented as shown in Figure 35 below

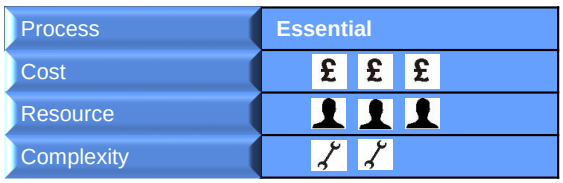

Figure 35 - FRACAS Process Intensity

7.2.5 FRACAS Checklist

- ✓ Has the correct team been identified?
- ✓ Has the failure been observed correctly?
- ✓ Is the correct documentation in place to record all failure details?
- ✓ Has the failure been verified?

- ✓ Has the failure been isolated?
- ✓ Has the failure been correctly analysed?

7.2.6 Further Reading

RD.15/000875.1: Failure Reporting, Analysis and Corrective Action System (FRACAS)

8 Recommendations for further work

In Phase 1 of the TiPTORS programme a detailed review has been undertaken of the potential processes that can be brought together across the 6 stages of a tidal turbine product development cycle from Design to Monitor & Control. As outlined in this summary report these have been brought together to establish a Design for Reliability (DfR) process, focused specifically on Tidal Turbine powertrains

The individual processes assessed have been reviewed for their "Process Intensity", that is to say the effort that would be required to successfully undertake each process. In addition, guidance has been provided as to how 'essential' an individual process is for assessing reliability, given the limitations many tidal technology developers will have with respect to their own design resource availability.

However, in order to fully develop an industry-wide, bespoke DfR methodology that can be used across a wide range of tidal technologies, it will be necessary to test the methodology by aligning the outputs from this phase to the tidal developers own design processes, with the following objectives:

- To map the DfR methodology in this report to the tidal developer's own design processes;
- Carry-out some of the "essential" steps for the tidal developer (e.g. FMECA, Reliability Growth etc.), working in partnership;
- Identify areas of the process that require further tailoring for tidal turbine technologies;
- Collate any useful data that currently exists to validate any future reliability simulation tool;
- Identify gaps in understanding of the "Physics of Failure" and where the ORE Catapult could create "spin-out" projects to fill these gaps (e.g. component testing); and
- Confirm data gaps and where the ORE Catapult could improve data collection through the development of enhanced sensor techniques aligned to the right failure modes.

Our recommendation is that the above objectives are carried out through "Pilot Projects" with the tidal developers working in partnership with the ORE Catapult and core capability providers such as Ricardo. It is proposed that at least 3 Pilot Projects should be undertaken with 3 different tidal technology developers, to allow for the outputs to then be collated into a bespoke methodology and a comprehensive gap analysis of the Physics of Failure and data requirements.

The DfR methodology would also be further enhanced by the creation of a Design Simulation Tool, developed by DNV GL, as outlined in the separate report (**PP124801-WP1.5-001**).

In conclusion, it is recommended that the Phase 1 work is progressed through a follow-on programme that trials the DfR methodology and ensures alignment with industry. The final output of such a programme would result in the following bespoke deliverables for the tidal industry:

- A bespoke and tested DfR methodology for tidal turbine powertrains;
- Deeper understanding of the Physics of Failure with clear recommendations of further sub-system and component testing;
- Enhanced sensor techniques to allow for improved data collection aligned to failure modes;
- A tidal turbine powertrain reliability simulation tool, validated through existing and new data input; and
- Enhanced certification process that addresses tidal turbine powertrain reliability.

Through these deliverables, the authors of this report are confident that the tidal industry will have an enhanced level of reliability, lower operation and maintenance costs and opportunities for design optimisation, resulting in a significant reduction in Cost of Energy.

Additionally, the enhanced certification process can also ensure that future tidal projects that follow the improved DfR methodology, benefit from reductions in insurance and finance premiums that would inevitably ensue, as well as provide high confidence for the investment community to support the sector. These effects would serve to lower the Cost of Energy further and help establish an attractive and buoyant tidal energy industry for the UK as a whole.

Contact

ORE Catapult
Inovo
121 George Street
Glasgow, G1 1RD

T +44 (0)333 004 1400
F +44 (0)333 004 1399

ORE Catapult
National Renewable Energy Centre
Offshore House
Albert Street, Blyth
Northumberland, NE24 1LZ

T +44 (0)1670 359 555
F +44 (0)1670 359 666
Info@ore.catapult.org.uk

ore.catapult.org.uk