RISK MANAGEMENT PLAN

Design, build and test of novel, remote, low-power wave energy converter for non-grid applications,
July 19, 2019

WORK PERFORMED UNDER AGREEMENT

DE-EE0008627

SUBMITTED BY

Columbia Power Technologies, Inc.

236 East High Street

Charlottesville, VA 22902

PRINCIPAL INVESTIGATOR

Ean Amon

Office: 541-368-5033

Fax: 541-230-1498

amon@columbiapwr.com

SUBMITTED TO

U. S. Department of Energy
Golden Field Office
Federal Project Manager: Yana Shininger
Federal Project Manager E-Mail: Yana.Shininger@ee.doe.gov

TABLE OF CONTENTS

TABLES

1 RISK MANAGEMENT PLAN

For the design of the Low-Power WEC, a Failure Modes, Effects, and Criticality Analysis (FMECA) will be performed to systematically identify all potential failure modes and their effects on the system. This analysis is incorporated early in the development cycle such that the mitigation of the identified failure modes can be achieved cost effectively and efficiently. The FMECA can begin once there is enough detail to functions and failure modes of a given system, and its interfaces with other systems. The FMECA occurs coincidently with the design process and is an iterative process which allows for design changes to overcome deficiencies in the analysis. The process is performed by a team of experts qualified to estimate the expected occurrence, magnitude and consequences of failure modes and design inadequacies. The collaborative team effort stimulates the thought process and ensures a thorough analysis for each system, failure mode, and operating mode. The areas of design expertise may include electrical engineering, mechanical engineering, controls engineering, systems engineering, software engineering, naval architecture, industrial manufacturing engineering, environmental engineering and maintenance operations support.

Columbia Power has adopted an FMECA plan tailored to meet the specific needs of the design, build, manufacturing, deployment, commissioning, and operation of the Low-Power WEC. The FMECA methodology described below follows IEC 60812 [1]. Additional guidance was taken from [2]–[4]. Furthermore, this Risk Management Plan is in compliance with the Risk Management Framework developed by the National Renewable Energy Laboratory [5].

1.1 Analysis Procedure and Expected Results

The FMECA follows a four-step process of identification, evaluation, classification, and determination of criticality as follows:

a) Comprehensive identification of potential failures modes which would have undesirable effects. Failures are detailed with respect to the systems functional hierarchy.
b) Evaluation of the likely cause(s) for each identified failure mode, as well as the effect. Unique combinations of failure mode and failure cause are registered and analyzed separately, as both the expected rate of occurrence and recommended actions to mitigate the risk will generally be different.
c) Classification of the registered risk item with regards to severity and probability of occurrence. Engineering design and preventative detection that reduces the likelihood of failure is considered in assigning an occurrence rating. Logistics and assets required for repair are considered in assigning severity ratings.
d) Determinations of the risk ranking of each registered risk item. Rankings are determined separately for each of the four severity classes: human safety, environment, WEC operations and assets.

Results from the analysis allow for improvements in reliability and reduction of risk as follows:

a) Allow for external experts to review and assist with risk assessment of the WEC system.
b) Allow for system design improvements to increase system reliability, maintainability and safety.
c) Allow for design improvements which enhance the maintenance, repair and operation (MRO) of system.
d) Ensure that the systems satisfy the project milestone requirements and system engineering design requirements.

1.2 Scope of FMECA

The FMECA covers the major WEC system, subsystems, and auxiliary system categories which support the function and performance of the WEC; this includes both the technology (e.g. power-take-off) and the project as a whole (e.g. permitting). The FMECA begins with the establishment of the rules for the analysis process as described in this document. The process includes executing the FMECA worksheets coincidently with the design process. The FMECA worksheets are used to record the results of the analysis. The results are reviewed and analyzed by the design team in an iterative process which is summarized in the design report with conclusions and recommendations. As the design development activities progress the FMECA is updated accordingly.

1.3 Description of Project Support

The FMECA for the WEC system supports the design process and design conclusion for each component, subsystem and system. The analysis allows a broad range of experts to review the risk implications of system design with respect to the success of the project. The iterative process allows for early identification of costly design deficiencies. The layered FMECA process helps identify unacceptable design combinations which could result in negative operational effects. FMECA conclusions will identify if there is a need for better component selection or redundancy, leading to improved design revisions. The analysis of the detection methods and diagnostics ensures that failures can be properly detected, and corrective measures are made.

1.4 Revisions, Scheduling, and Document Control

Revisions will be performed as part of the design review process. During the design process, the risk spreadsheet is updated by the system owner for each major design change. The system owner is responsible for completing the FMECA and presenting it during the design review where the FMECA worksheet and the design are reviewed. Revisions are tracked by the system owner.

All systems are regularly reviewed to establish focus groups to reduce highest risk areas. The orchestration of the overall WEC FMECA program is performed by the system owner of the risk management plan.

1.5 Identification, Mitigation, and Closure of Action Items

The FMECA worksheet is designed to establish an accurate risk ranking system which allows for the cross comparison and sorting of items in the risk register. The worksheet collects the risk details and is used to rank them into one of three risk status level for each risk; tolerable, undesirable and intolerable. For brevity's sake, these are sometimes referred to as low, med (medium) and high. Intolerable risks are not acceptable, and the design is iterated until a reduced status is established. Undesirable risk items require consideration of engineering actions that would reduce risk; when considering tradeoffs between increased cost/complexity and reduced risk, it may be justifiable to accept an undesirable risk item. A risk classification of tolerable does not require any further engineering action. Engineering actions recommended to mitigate risk are recorded in the worksheet, as are actions taken along with updated occurrence, severity and risk rankings. Once a tolerable or undesirable risk is finally accepted, the status of the registered risk item is changed from open to closed.

1.6 Risk Management Process Overview

The following sections are a general overview of the process of performing risk analysis for the Project. The risk analysis is an iterative process which progresses with the design maturity.

I. Risk Analysis Process Review

The methodology used for FMECA risk analysis is described in this document and executed for each system with the FMECA worksheets. This risk analysis process is reviewed at the outset of the project by the project team.

II. Risk Identification and Analysis

The risk analysis is developed with FMECA worksheets by Columbia Power engineers.

a) Each system engineer preliminarily identifies and assesses the risks applicable to that system, with knowledge gained from industry experts through the design process
b) Multi-disciplinary team of engineers performs additional risk identification and analysis. This is a collaborative process including engineers not directly involved in system design or development.
c) Industry experts (i.e. Maritime Markets Advisory Board (MMAB) members are solicited for additional risk identification and analysis

III. Review and approval

a) System owner peer review
b) Engineering management review and approval
c) Corporate review and approval
d) Iterative refinement of FMECA – steps II and III are repeated until all risk items have been identified and risk reduced to an acceptable level. Design changes initiate further risk iterations.

IV. Final release

a) FMECA is used to guide engineering and operations

2 WEC SYSTEM INFORMATION

The WEC is divided into systems and subsystems; for each major system and subsystem the system engineer identifies risk items and performs a risk analysis using the standardized FMECA worksheet. The systems are described with appropriate detail such that all parties can contribute to the risk analysis. The system description can consist of the following information, as appropriate:

- List of system components and functions
- System functional block diagram
- Interface Control Documents (ICDs)
- Redundancy level
- Position and importance within WEC
- Inputs and outputs (I/O) of system

This information is contained, or referenced, in the system Design Document.

3 FAILURE MODE, EFFECTS, AND CRITICALITY ANALYSIS (FMECA)

The FMECA is a bottom up analysis which uses a hierarchical approach starting at the lowest individual failure mode and working up to the overall system effect. The analysis begins with the item failure mode and causes. The failure is evaluated at all levels, from the component function to the end effect on the system. Such effects may include a reduction in performance or need for maintenance and repair.

3.1 Definition of System Boundaries

The ICD describes and details the systems interfaces at the boundaries with other systems. In addition to the ICD, a system functional block diagram or other relevant schematic shows interaction of the cascading effects of failures across systems. Boundaries are defined by their input and output functions. Related components that lie outside of a system boundary may be explicitly mentioned as excluded from the analysis to ensure items are not overlooked. Components inside the system can be further analyzed with the use of the functional block diagrams, P&ID or other relevant schematic.

3.2 Level of Analysis

The systems are broken down by function and components and assigned a level of hierarchy. The highest level is defined by the system concept and its specified input and output requirements. Commercial off the shelf (COTS) products used for their intended function are generally considered at a high level of maturity with respect to function. COTS components used in a novel manner, prototype components or configurations are analyzed in more depth. These concepts are covered by the Technology Class ranking, see [3] and [6]. Maintenance, repair, and operation (MRO) also contribute to a systems maturity level by considering the effects of an associated failure.

3.3 System Functional Diagrams

System structures may be represented with functional block diagrams for internal system components and with ICD diagrams for system interfaces as required. P&ID or other schematics may also serve the purpose. System diagrams may be useful to show all series connections, redundancies, and functional interdependencies.

3.4 System Commissioning, Initialization, Control, and MRO

The status of system and configurations during all operational modes should be specified, including system commissioning, initialization, and MRO. Changes in the level of risk are analyzed with consideration of minimum system performance for each operational mode. Specific requirements for minimum system performance level are developed with accurate knowledge of the following:

- Duration of system function and time interval between operations.
- Time allowed for corrective action before serious consequences.
- Necessary personnel and interactions by operators.
- Start-up, shut-down and transitional modes.
- Control during operational phases.
- MRO operations required.
- Testing procedures to verification of operation.

3.5 Failure Mode Determination

All operational modes should be considered when determining possible failure modes for a system or component. For each system, different operating conditions and changes in configuration should be specified. A failure in one particular operational mode and associated configuration may be more critical than another.

A list of general failure modes should be considered for the determination of item failure modes, causes and effects. The following topics are analyzed for the development of the general list of system failure modes.

- Use of the system.
- Item, element, component or part of the system involved.
- Configuration or mode of operation.
- Operational prerequisites and specifications.
- Time and space constraints.
- Environmental stresses.
- Operational stresses.

Items from commercial suppliers should have identified failure modes, however if the manner of which the product is used varies from normal, additional failure mode analysis is required. The method of failure, resultant operational condition of the failure, and diagnostics available for the component should be considered. The remedial actions for the failure of a component should be well understood for system diagnostics and fault recovery.

3.6 Failure Causes

Failure modes may have multiple potential causes. The most likely failure cause(s) should be identified for each failure mode. Identification and description of all failure causes is not always necessary. The level of description, identification and mitigation of each failure cause should be based on the severity of resultant failure mode. The most severe failures modes would have the highest level of failure cause analysis. Recommended mitigation actions are evaluated based on the level of risk. Common Cause Failures (CCFs) are a typical part of the failure analysis. Some CCFs include software bugs, components ratings, environmental conditions, interference, vibration, and human influence. Redundancy, identification of common tests, and preventative maintenance are all used to overcome CCFs.

3.7 Failure Compensation Methods

Methods for failure compensation are identified as any means to prevent or reduce the effects of the failure mode. Compensation ability is clearly described and recorded in the FMECA. Failure compensation should consider the following methods:

- Redundant items allow for continued operation in the case of the single failure.
- Monitoring, alarms and detection methods to isolate and prevent high risk failures.
- Alternate operational configurations or modes in case of failure.
- Quality control
- Scheduled inspection and maintenance

3.8 FMECA Worksheet

For each system an FMECA worksheet populated by the system engineer with peer reviewed risk identification feedback from a multidisciplinary team of experts. The FMECA system risk items are added to and analyzed by the group for each stage of the design development. As the design matures, each system design change prompts additional risk analysis. The tables defining the rankings for occurrence and severity, as well as the risk ranking, are shown in the Appendix – Occurrence, Severity and risk. This section describes all FMECA table entries.

3.8.1 Risk ID

The risk identifier is a serial number which starts with the subsystem number, with the number of the risk item suffixed. For example, “0111-1” is the risk ID for the first risk identified for the specific subsystem (0111) in the hull system (0100). The risk identifier allows for unique identification of all registered risk items, as well as sorting by system and component.

3.8.2 Item Description

A description or name which describes the system or component entered for the risk analysis.

3.8.3 Function

Enter a description of the primary function(s) of the item with regards to the system or project. The functions should match those identified in the Technology Assessment worksheet.

3.8.4 Technical Class

Identifies the novelty of the component in terms of the technology and the application. It is a numerical value from 1 to 4 and should match the value in the Technology Assessment worksheet. Technology Assessment framework, along with the description of technical class, is described in [3].

3.8.5 Novel Aspects

A brief description of the novel aspects of the technology and/or application. This should match what is stated in the Technology Assessment worksheet.

3.8.6 Failure Mode

Enter a general title for the basic failure (mode) of the item (i.e. snapped mooring line, seized bearing). There can only be a single failure mode per line item

3.8.7 Failure Effects

List the failure effect(s) of failure mode for the item.

3.8.8 Failure Causes

Enter a potential cause for the failure mode. For each potential cause identified and registered, enter a new line item for the item's failure mode. The item description, function, technical class, novel aspects and failure mode are duplicated for each new potential cause. Each cause has a separate risk, therefore a separate line item. If a failure cause applies generically to all equipment or a group within a system or subsystem, then that cause and mode are kept at the highest practical level of analysis and the severity is assumed to be the worst-case possible severity and worst-case occurrence for those affects.

3.8.9 Initial Mode of Operation

State the initial mode of operation prior to the failure occurring. Different initial modes of operation have different levels of risk. Add additional line items for other modes of operation as necessary.

3.8.10 Risk Reduction Design

Enter design techniques, methods and controls implemented to reduce the risk to the system or project caused by the potential failure of the line item.

3.8.11 Preventative Detection

Enter what indicators there are of a potential item failure, the method of detecting the indicator, and the means by which the failure is avoided, or failure effects are reduced, by either automatic or manual controls or maintenance.

3.8.12 Post Failure Detection

Enter the method by with the failure and/or failure effects are detected after the failure has occurred. It is desired to be able to detect and correctly identify an item failure with remote methods.

3.8.13 Post Failure MitigationStrategy (automated, manual)

Enter the method or strategy for repairing the failed item or reducing the failure effects once the failure has occurred.

3.8.14 Occurrence

For a prototype the determination of probability of occurrence is a qualitative analysis where estimation is based on engineering experience about known existing commercial systems. In most cases prototype failure occurrence specifications are not readily available. It is important to consider the operational profile with regards to environment, electrical, or mechanical stresses which contribute to the probability of occurrence. The ranking of occurrence is shown in the Appendix in Table 1. The occurrence often correlates exponentially to increased operational stresses. The probability can be estimated with consideration of the following:

- Component life testing data
- Failure rate databases of field testing.
- Failure data and rates from similar items
- The life or time period for which the item is used
- Environmental stresses

- Engineering judgment

Engineering design and preventative detection that reduces the likelihood of failure is considered in assigning an occurrence rating.

3.8.15 Severity

The severity rating is used to identify how serious the effects of a given failure mode are. The severity is rated from insignificant to catastrophic (see Table 2 of the Appendix). The severity of a failure can affect the system, environment, or humans in a number of ways, therefore severity is considered with regards to four classes;

- Human Safety
- Environment
- Operation
- Assets

Logistics and assets required for repair are considered in assigning severity ratings.

3.8.16 Risk Ranking

The risk ranking is based on the occurrence probability rating and the severity rating for the four classes of severity. The risk ranking can be reduced by an engineering a design change which reduces the probability of occurrence or reduces the severity of the failure. The risk rankings are presented as a look-up in Table 3 of the Appendix.

3.8.16.1 Intolerable (High)

Risk items with intolerable risk ranking are identified as having an unacceptable level of risk to the system during the lifetime of the project. Intolerable risk rankings correlate to major, critical, and catastrophic failures which have a more than moderate chance of occurring. Minor failures with a very high probability of occurrence are also considered intolerable. Intolerable risk items are analyzed and engineered until a lower risk status is achieved. For brevity, high is synonymous with intolerable.

3.8.16.2 Undesirable (Med)

Undesirable risk ranking is a lower level than intolerable and signifies failures which may or may not require further engineering design changes to reduce the risk. All undesirable risk items are reviewed by corporate and the design team to determine if further engineering action is required to mitigate risk. The outcome of the review is documented on the FMECA worksheet including what engineering action will be taken, if any. Some undesirable failures may be unavoidable or have solutions which are beyond the project's time and financial allowances. For brevity, medium (med) is synonymous with undesirable.

3.8.16.3 Tolerable (Low)

Tolerable risks are identified as having an acceptable level of risk to the system during the lifetime of the project. Tolerable failures can be catastrophic in nature if there is only an extremely remote chance of occurrence. Conversely, a failure with a very high probability may be tolerable if the resultant effects are of very low significance. Risk items with a tolerable status require no further engineering design revisions to improve their risk status. For brevity, low is synonymous with tolerable.

3.8.17 Recommended Actions

In this section describe engineering, design, maintenance, repair, or operational recommendations for the risk reduction of the line item. Include suggestions for systems design, data acquisition, and research topics which relate to the further reduction in risk. This column is optional; if no actions are recommended it can be left blank.

3.8.18 Responsible Party

Identify the party responsible for the risk reduction activities identified in “recommended actions”.

3.8.19 Actions Taken

This section lists the steps toward item risk reduction which have been completed since the initial line item entry. The list of action items is a record of design changes or document additions to mitigate risk.

3.8.20 Updated Risk Ranking

If actions were taken to mitigate risk, an updated assessment of occurrence, severity and risk rankings is documented here.

3.8.21 Recommended Actions (2^{nd})

If the updated risk ranking is undesirable or intolerable, a 2^{nd} set of risk reducing actions may be recommended. If so, responsible party (2^{nd}) and actions taken (2^{nd}) are also documented.

3.8.22 Additional Updated Risk Ranking

If additional sets of actions were taken to mitigate risk, updated assessments of occurrence, severity and risk rankings is documented here.

3.8.23 Status

The status column is for indicting whether a line item is open or closed. The status clearly indicates when a decision to accept the level of risk and close the line item has been made.

3.8.24 Notes

Enter any questions, comments or uncertainties. Notes are looked at during design review.

3.9 Notification Guidance

The FMECA process occurs coincidentally with the design and development process. Notification and guidance will consider time, resources, and scheduling to allow for proper and timely risk feedback into the design process.

3.10 Review Process

The initial risk register item entry and review occurs iteratively with the design development. The multidisciplinary team and system engineers populate items of risk and perform an analysis for each stage of design development. Once the risks are documented and analyzed, an internal team review is performed. Where appropriate, industry experts from outside of Columbia Power will be engaged for further review.

3.11 Reporting

In addition to the completed FMECA worksheets, the risk analysis process and results are documented in the system Design Document.

4 REFERENCES

[1] "Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)," IEC 60812, 2006.

[2] "Procedures for Performing a Failure Mode, Effects and Criticality Analysis," Dept of Defense, MIL-STD-1629A, 1980.

[3] "Qualification of New Technology," Det Norske Veritas, DNV-RP-A203, 2011.

[4] "Guidelines on Design and Operation of Wave Energy Converters," Det Norske Veritas, 2005.

[5] D. Snowberg and J. Weber, "Marine and Hydrokinetic Technology Development Risk Management Framework," National Renewable Energy Laboratory, NREL/TP-5000-63258, Sep. 2015.

[6] "Certification of Tidal and Wave Energy Converters," Det Norske Veritas, DNV-OSS-312, 2011.

5 APPENDIX – OCCURRENCE, SEVERITY AND RISK

Use the following tables to complete FMECA worksheets for each system and topic

5.1 Occurrence

The expected annual failure rate of the identified failure mode is rated from 1 to 10.

Table 1 – Occurrence

Rating	Occurrence	Annual failure rate	Return period [years]
1	Exceptionally unlikely to occur	0.0000100	100000
2		0.0000316	31600
3	Extremely unlikely to occur	0.000100	10000
4		0.000316	3160
5	Very unlikely to occur	0.00100	1000
6		0.00316	316
7	Rarely expected to occur	0.0100	100
8		0.0316	32
9	One or more during 20 yr lifetime	0.100	10
10		0.316	3

5.2 Severity

The severity of the failure effect is rated from 1 to 10, with respect to human safety, environment, WEC operation and assets.

Table 2 – Severity

Rating	Severity	Human Safety	Environment	WEC Operation	Assets
1	Insignificant	Negligible injury, effect on health (e.g. band aid)	Negligible pollution or no effect on environment	Negligible effect on performance	Negligible
2					[1.5k USD]
3	Minor	Minor injuries, health effects (e.g. stitches)	Minor pollution / slight effect on environment (min disruption on marine life)	Minor system degradation	Repairable in-situ, at next maintenance interval [3k USD]
4		Moderate injuries and/or health effects (e.g. broken bone)		Moderate system degradation (e.g. loss of function, repairable in-situ)	Repairable in-situ, outside maintenance interval (1 day) [5k USD]
5	Major		Limited levels of pollution, manageable / moderate effect on environment		Repairable in-situ, outside maintenance interval (1 week) [15k USD]
6				Major system degradation or loss of operation for 1 month	[25k USD]
7	Critical	Hospitalization (with full recovery)	Moderate pollution (some clean-up costs) / Serious effect on environment	Major system degradation or loss of operation for 3 months	Dry dock required for repair [50k USD]
8				Critical system degradation or loss of operation for 6 months	[150k USD]
9	Catastrophic	Hospitalization (with lasting disabilities)	Major pollution (significant clean-up costs) / disastrous effects on the environment	Failure to generate power for remainder of project, complete failure	Loss of device [500k USD]

10		A fatality			

5.3 Risk Ranking

The risk ranking is determined by using the following table. Low, Med and High risk rankings correlate to Tolerable, Undesirable and Intolerable (see 3.8.16).

Table 3 – Risk rankings

	Severity									
Occ	1	2	3	4	5	6	7	8	9	10
10	Low	Med	Med	Med	Med	High	High	High	High	High
9	Low	Low	Med	Med	Med	Med	High	High	High	High
8	Low	Low	Low	Med	Med	Med	Med	High	High	High
7	Low	Low	Low	Low	Med	Med	Med	Med	High	High
6	Low	Low	Low	Low	Low	Med	Med	Med	Med	High
5	Low	Low	Low	Low	Low	Low	Med	Med	Med	Med
4	Low	Low	Low	Low	Low	Low	Low	Med	Med	Med
3	Low	Low	Low	Low	Low	Low	Low	Low	Med	Med
2	Low	Low	Low	Low	Low	Low	Low	Low	Low	Med
1	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low