DEEP LIFE OPEN REVOLUTION FAMILY OF REBREATHERS

FAILURE MODE, EFFECT AND CRITICALITY ANALYSIS VOLUME 3:

Electronics MTBF, MTBCF and preventative maintenance

DOCUMENT NUMBER: [Filename]	FMECA_OR_V2_Elec_MTBCF_090529
ORIGINATOR:	**Review team comprising Dr. Alex Deas, Igor Abrosimov, David Coyne, Marat Yevtukhov, Alexei Bogatchov, Dr. Bob Davidov, Dr. Vladimir Komarov, Dr. Oleg Zagreblenny,**
DEPARTMENT:	**Engineering**
DATE:	**29th May 2009**
REVISION:	**D1**

APPROVALS	
___/AD/_____ Project Manager	__29th May 2009_____ Date
/VK/_____ Quality Officer	__29th May 2009_____ Date

Controlled Document ☒   Classified Document ☐
when RED   **DO NOT COPY.**

Revision History		
Revision	**Date**	**Description**
A	11th Nov 2005	Document assembled from other files
B	30th Jan 2006	MTBF and MTBCF Passed Review
C	27th Mar 2006	Additional action after He pressure tests, batteries.
D	3rd Jan 2007	Update based on test results. Clarified Method.
D1	29th May 2009	Updated.

Copyright © 2006, 2007, 2009 Deep Life Ltd

This document is maintained on a SVN source control system and is under Revision control. The Revision Number is marked on every page, along with the date of the entire document. The Revision Numbering comprises an Alphabetic Letter (A, B, C, D, etc) for all major rewrites, and a letter for edits of sections of this document (0, 1, 2, 3, etc). Where an update is made that does not involve reissue of the entire document, then the Revision History sets out which pages are affected.

Table of Contents

1 PURPOSE AND SCOPE

This is Volume 2 of the FMECA of the Deep Life Open Revolution Submission, Project ORECCR1. This document covers the MTBF and MTBCF of the electronic circuits in the rebreather. The MTBF of the mechanics is described by a separate document.

This is a review document, with design changes highlighted, to achieve the target performance. The result is Circuit Diagram Revision C1.

The circuit diagrams accompany this document. For completeness, these are in the form of Submission A, Submission B and Submission C. Submission A is the circuits submitted to the review team, and Submission B is the same circuits with the decisions from the review implemented. The changes between Submission B and C improve the MTBCF to meet the design intent.

> **It should be noted that Submission B fails the MTBCF review, and Submission C passes. Present revision is Submission C, and all observations are implemented in circuit revision D0.**

2 METHOD AND CONFIDENCE LIMITS

The method used to calculate MTBF is that of MIL-HDBK-217F Parts Stress Method. This is the most rigorous of the MTBF calculations in common use. Assumptions involving managing redundancy are according to EN 954. Review includes the provisions and processes of IEC 61508 subparts 0 to 7.

The raw MTBF or FIT data is taken from manufacturers. In most cases, the MTBF is to 60% confidence whereas for the present purposes, data with 90% confidence is preferred. To fill this gap, multiple batch MTBF data is used.   For example, data from National Semiconductors is taken every 6 weeks and the component has been in production for a number of years: the Design Team specifically avoid new components where ever possible. Each batch of components is tested by National Semiconductor, and the MTBF figures are available. The size of the batch and the duration of the test is chosen by National Semiconductor to give the 60% MTBF confidence, at an ambient temperature of 50C. Taking data from two batches increases the confidence to 80%, 4 batches to 90%. In a majority of cases the test batch have zero failures, so the actual MTBF may be considerably better than that determined by the test.

The environmental conditions were considered carefully. The operating temperature of the components in the system is generally well below 50C, and this provides a further margin of safety as MTBF of all components is known to reduce with increasing temperature.

None of the components are stressed electrically beyond their designed operating points.

There is a specific hazard from helium penetrating components and causing their failure. To overcome this hazard, all component types were tested in pure helium at 141bar in a series of tests lasting from 21 days to 3 months. Components that exhibit significant changes in characteristics in this environment were eliminated from the design, except for the clock oscillator which was chosen to have very low helium migration characteristics, batteries which were moved to outside the rebreather into a sealed chamber that can withstand their vapourisation, and pressure sensors for which a helium resistant design has been produced. It is noted that all piezo electric and all piezo resistive components tested failed in pure helium. The results of the helium trial is published as a separate design verification report, ***DV_Helium_soak_060511.pdf***, available from the Deep Life Ltd web site.

3 FAILURE MODES FOR MTBF CALCULATIONS

The HAZOP procedure as defined in QP-23 was applied hierarchically, down to the individual component level. The conclusions are recorded below. The source data is available and is published for peer review.

3.1 Inductors

Inductors are used for buck converters in the 5.5V power supplies (L1 and L2 on Power Card, 10uH), and also as filters for data over power (L1, L2, L3, L4 100uH on Base Card).

The power inductors can fail only in the open state. This means the entire power supply circuit around U1 and U2 on the Power card, can be treated as mutually redundant (with the proviso on replacement of the tantalum capacitors in Section 2.3).

Failure of the Base Card inductors is not critical because it causes loss of communication with the handset, if it occurs at the same time as the optical communication channel fails, but the entire handset can be unplugged and the unit still operates normally using either the FPGA or the Microcontroller in the Base Card. For this reason, the Base Card inductors need not be in the MTBCF calculation but are in the MTBF calculation, though for safety, they are included in both calculations. These inductors act in a circuit with triple redundancy so the overall effect on the MTBCF is negligible.

3.2 Ceramic Capacitors

Ceramic capacitors across power supplies fail with a short or an open. If these fail with a short, then the FITs must be added and these act as common parts, reducing the overall MTBCF considerably. To avoid this, these capacitors are 0603 parts, with the power supplies able to blow them if they fail with a short. In this case, these capacitors are mutually redundant.

3.3 Tantalum Capacitors

Tantalum Capacitors have a FIT figure from 5 to 10 failures per billion hours depending on their stress, with 90% of failures being short circuit. This is a problem for power supplies which are themselves redundant. For example, C16 and C19 are the smoothing capacitors on the output of the 5V regulators (U5 and U6 on Page 1 of the Power Card Circuit). For these two capacitors alone, the combined FIT would be one in 50 million hours: just these components alone if not protected would prevent the unit achieving a 1 billion hour MTBCF target. This means the Tants across power supplies must be replaced by large value ceramic capacitors, which have a FIT of under 0.1 per billion hours.

As a result of this determination, in Rev B an Rev C designs, all Tants in common circuitry were replaced by ceramic, and the risk of parallel mode failures mitigated by using small devices for the value (so the device will fuse if it fails as a short).

3.4 Logic Gates

The failure of a particular gate is the FIT for the part divided by the number of gates. Failures at 1 and 0 are assumed to be of equal probability.

For the EXOR gates used to switch out failing clocks, such as U42 and U43 on the Base Card page 12, the FIT is halved, because only a failure in a 1 state can propagate to become a critical failure.

3.5   Power Supply Integrated Circuits

The worst case of U1 and U2 on the Power Card was considered. The FIT of these two boost converter regulators is 1.66. Failure of this circuit, will lose just the ADCs and the stepper motors and all other circuitry is supplies by 3.3V or below (when U1 and U2 on the Power Card fails, then the battery voltage of 2.7V to 3.3V appears on the 5.5V rail, minus the drop across two Schottky diodes).

The FIT of 1.66 is for the converter under operational stress. For the converter on standby, the FIT is reduced by a factor of better than 10. Therefore, this converter circuit needs to be changed such that the circuit can withstand any failure mode, and one converter is always on standby.

Action: Add a second Schottky diode between the anode of D2 and R20, so when the converter fails in a short, it does not take down both power supplies, and similarly on D7 and R21, on the Power Card. Use the controller to ensure one circuit is on standby, unless then primary converter fails.

The current consumption health monitor circuit around U8, is not a critical function except for R18.

Action: Two resistors should be fitted in parallel instead of R18, as the FIT of 0.202 eats away too much from the common device budget in their present configuration.

Confirmed that both of the above actions were carried out for circuits Rev B and C.

3.6   2.5V Reference

This is used for the scrubber stick CO_2 reference and scrubber life monitor. This reference is actively monitored, and if the reference fails, then the reference will be 3.3V or 0V. In the case of 3.3V the digital circuitry can manage the failure, in the case of a 0V failure, the circuitry will detect the failure, continues to monitor WOB and PPO2, but instructs bail out. This is not a critical failure, because no rebreather in current use has the capability to monitor PPCO2 or scrubber life accurately anyway.

3.7   Non-critical blocks: Charger, USB, Handset

None of the above functions are needed for the unit to operate safely, therefore these are in the MTBF figures but not MTBCF.

3.8   Optical Fibre

This has redundancy using the data over power lines.

Failure of the Optical Fibre or circuitry is not a critical failure, because the handset still calculates Deco, as does the HUD, the Base Card still controls PPO2, PPCO2 and WOB.

3.9   Clock Circuitry

Failure of a clock, is a critical failure if there is no redundancy. For example, in most existing rebreathers, if the system loses the clock will cause a handset to hang, no alarms, the display has a 50% probability of still being readable, no handover to a slave handset, and no O2 injection.

To prevent this failure, the following measures are taken:

The FPGA uses different buffers to the microcontroller. Either microcontroller or FPGA can run the system. Use of two completely independent clocks introduces risk of synchronization failure, therefore two clocks are provided but only one is used: that is the clocks are mutually redundant.

The 8MHz clock redundancy circuit uses a monostable (U34 and U35) to provide a cycle by cycle watchdog. One monostable is in standby all the time, being continuously reset by the active monostable. The FIT of the inactive circuit is improved by a factor of 10 compared to the active circuit. The clock output from the non-blocked monostable is then combined with U42 and U43 to give a single clock. The NOR gates combining the clocks are arranged to be in different packages, and the key part, U47 is a high reliability device rather than the common 74HC series part.

The 31.25KHz clock is used to measure ambient pressure. This clock is redundant, because the same data is available from the handset. Therefore the failure of the 31.25KHz clock is the failure of those components, with redundancy of the whole handset.

The 1MHz and 62.5KHz clocks are not essential for the regulators that use it: they oscillate themselves if there is no clock. The 1MHz clock is provided to avoid power supply noise affecting the ADC values. The ADC operates within critical safety limits, though with less accuracy, if this function is disabled.

Oscillator components are chosen that have a very low helium migration figure. The components are in a chamber filled with silicone oil and sealed from the breathing loop. The helium appears not to migrate through silicone oil: helium migration occurs through the stress lines in the material – materials not under stress exhibit helium migration rates many orders of magnitude less than for materials under moderate stress. To keep the helium out of the silicone oil, a stainless steel plate separates the oil from the breathing loop with a thermal expansion chamber into the breathing loop space, so the plate is not under stress. The breathing loop is maintained within 40mbar of ambient pressure so there should be minimal helium migration through the walls of the electronics chamber when the unit is operated in a saturation diving environment.

3.10 Shut off valve circuitry

The Shut Off Valve is a safety system which mitigates the effect of an otherwise critical failure. It is driven from the same sensors as the electronics above. This means that that electronics fails, so will the Shut Off Valve. Therefore the Shut Off Valve is excluded from the MTBCF calculation, but included in the MTBF, on the basis that if there is a failure of the circuitry then the shut off valve may fail as a direct consequence.

The Shut Off Valve is independent of the mechanical systems, so the MTBCF of the mechanical components in the breathing loop, are reduced to those between the Shut Off Valve exhaust and the exhale mushroom valve. This is considered in the FMECA review, document volume 2B.

3.11 Connectors

Connectors are treated as individual pins, with redundancy where this applies (i.e. where pins are connected in parallel but only one pin is required to carry the maximum current). Connectors use bifuricated sockets for reliable connection. Pins are hard gold plated over brass to protect from corrosion.

3.12 O2 Sensors

A full Safety Verification Study has been carried out on the O2 sensors as part of this design activity and is available to the reviewers : the intention is to publish that report in Q1 2007. This concluded that no sensor from any manufacturer met the requirements of the application.

Improvements were implemented by Analytical Industries to address the cause for their sensors failing assessment, by improving the mechanical robustness of the sensor, connector and changing the pcb design such that all failure modes where the sensor fails in a high state are eliminated – this requires the sensing circuitry to check the internal load

on the sensor is present and has the correct value. Only these approved sensors should be used with the rebreather. The firmware has been programmed to check for the correct sensor type based on the load characteristic, which as been chosen to be unique.

This leaves the O2 sensor as single sourced. Efforts should be made to assist a second manufacturer to improve their product to meet the requirements for this application.

O2 sensors are assumed to have a 12 months operating life, with random failure during this period of 10% of the population: this is based on data on Teledyne sensors which have the worst failure rates seen in any sensor measured by Deep Life Ltd. The Analytical Industries sensors seem to be much better but more time is needed to confirm this . Based on this assessment, to achieve the required MTBCF O2 sensors are in quadrature redundancy, and supplemented by a failure detection system involving predictive O2 injection.

The review team accepted the argument that this was sufficient to cover each of the seven credible failure modes, after examining the formal fault models and testing these in the formal specification (using Matlab).

3.13 Handset and HUD

A failure to signal to the user the PPO2 is not itself a critical failure. These are therefore excluded from the MTBCF calculation, but included in the MTBF. In reality, the Handset, HUD and Voice Annunciation work in triple redundancy, and the handset alone is billion hour compliant, so there effect of included or excluding the handset and HUD from the calculation is negligible.

3.14 Batteries

The batteries are actively monitored during rebreather operation and charging. Specific power up tests are applied, and predictive replacement is advised. This is expected to occur every 500 charges. One charge should last 10 dives if taken without a long gap between them.

The batteries are triple redundant.

The batteries are Lithium Ion Gel, which has been tested to withstand sudden pressurization and depressurization when in a silicone oil. During trials one battery did leak under helium pressure of 143bar. The unit is being qualified to 61bar. Therefore, the batteries must be in a one ATA chamber. The batteries take on helium and immersion in silicone oil as well as separation of the electronics from the breathing loop is required to keep the rate at which helium diffuses into the batteries to a low level.

Batteries have a high energy density and if shorted, can explode.

To prevent the batteries presenting a risk to the user or operators, the batteries have been moved to hermetic chambers located outside the rebreather and maintained at 1 ATA. The hermetic chamber is designed to contain the vapourisation of the batteries: a stainless steel tube with 1.5mm wall thickness is sufficient. The chamber is not a battery pack, but hardwired to short current and reverse limiting circuitry: the diode on the power supply is sufficient, coupled with the over-current limiting in the regulator attached directly to it.

3.15 Connectors

Two DIN 41612 connectors are used. The main failure mode is due to corrosion: there is very little risk of shorts between connector pins. This means each connector pin can be treated independently.

All critical connectors have redundant connector pins unless the item being driven is itself redundant, in which case the connector FIT is added to the FIT of the device at the end of the line.

Important but non-critical communication between the handset and Base Card uses both fibre-optic and electrical connectors for the operational reliability of this link.

4 PREVENTIVE MAINTENANCE SCHEDULE

4.1 Biohazards

The unit is cleaned using a strong bactericide every 12 hours of elapsed hours if the unit has been dived. The sterilisation schedule was reviewed.

The unit checks it has been cleaned by checking the hoses have been disconnected.

Full sterilisation procedure is issued with the product, using Virkron (daily) and PeraSafe (monthly). These are dental and surgical disinfectants compatible with the materials used in the rebreather and are available worldwide.

The manufacturers of Virkron advise that 10 minutes exposure is required to kill all bateria and viruses. If the system has 2 minutes wet exposure followed by a minimum 8 minute drying time, that would meet the 10 minute requirement – generally the drying time is much longer giving greater protectoin. PeraSafe is required monthly with a 10 minute soak.

Special attention is given to the hose design in the mechanical FMECA to avoid water laying in the hose loops, allowing bacteria to breed between dives. The entire design has been checked for drainage characteristics.

4.2 Scrubber

Test results for use at 100m, under conditions worse than EN14143:2003, indicate a scrubber life from 4.5 hours to 30 hours depending on type and configuration (single or dual scrubber, respectively, $Ca(OH)_2$ or LiOH).

The scrubber is actively monitored, and its failure is detected reliably using both a scrubber thermal capacity mode based on integrated thermal generation, gas density and gas flow. Gradual failure is ensured using a slightly non-uniform gas flow and a CO_2 detector is provided which fails safe (i.e. shows high CO_2). Routine replacement of the scrubber after every 4.5 hours of diving, with predictive scrubber life and health monitoring is acceptable.

Replacement checked by using a sensor to ensure scrubber is opened when user claims scrubber is replaced, is used to prevent the user opening the scrubber canister but failing to replace the scrubber.

The case of the user putting back a used scrubber is avoided by visibly damaging the scrubber when it is extracted: the procedure being advised it to use two cork screws supplied with the unit.

There has been a concern expressed over the risk of users fitting a damaged scrubber. If the scrubber is badly damaged, then CO_2 bypass will be very large and detected by the system as soon as it is used.

4.3 O2 Sensors

O2 sensors should be replaced annually.

The review team found the marking of date codes on the sensors to be inadequate: unclear, codified and too small. The label is redesigned with 10mm high characters with the date, and supplied with a set of labels the user can apply with the date the sensors are installed.

The review team noted fatal accident on 4/4/06 on a eCCR caused by the user failing to replace sensors and the electronics not testing the sensors.

4.4 IR source

The IR source has a 40k hours MTBF, replaced every 10K hours. The function of the CO2 sensor has redundancy with temperature stick, and failure of the source is detected for low risks such as the HC sensing and CO sensing.

4.5 Batteries

All batteries are actively monitored, and failure predicted when the battery fails to charge within a 50% tolerance of the new battery.

In addition to the above monitoring, batteries are subject to preventative maintenance replacement, and should be replaced every 300 charge cycles: their design cycle life is 500 cycles.

5 OVERALL MTBF AND MTBCF

The overall electronics MTBCF is 2.9 billion hours in the single scrubber configuration (2.9 x 10^9 hours), and 8.4 billion billion hours (8.4 x 10^18) in the twin scrubber configuration, with MTBF in excess of 800k hours.

The mechanics has a MTBCF of > 4 billion hours, but a MTBF of only 40k hours due to the seals around the scrubber. Mechanics MTBCF is reported separately: some further assessment of this is underway for confirm that the MTBCF assumptions are correct.

Full calculation of the electronics MTBCF and MTBF can be found in the accompanying Excel spread sheet, filename MTBCF Calc Rev C1.xls, with the overall result shown below for one scrubber. The twin scrubber system is simply the square of the MTBCF and half the MTBF, as it offers full parallel redundancy.
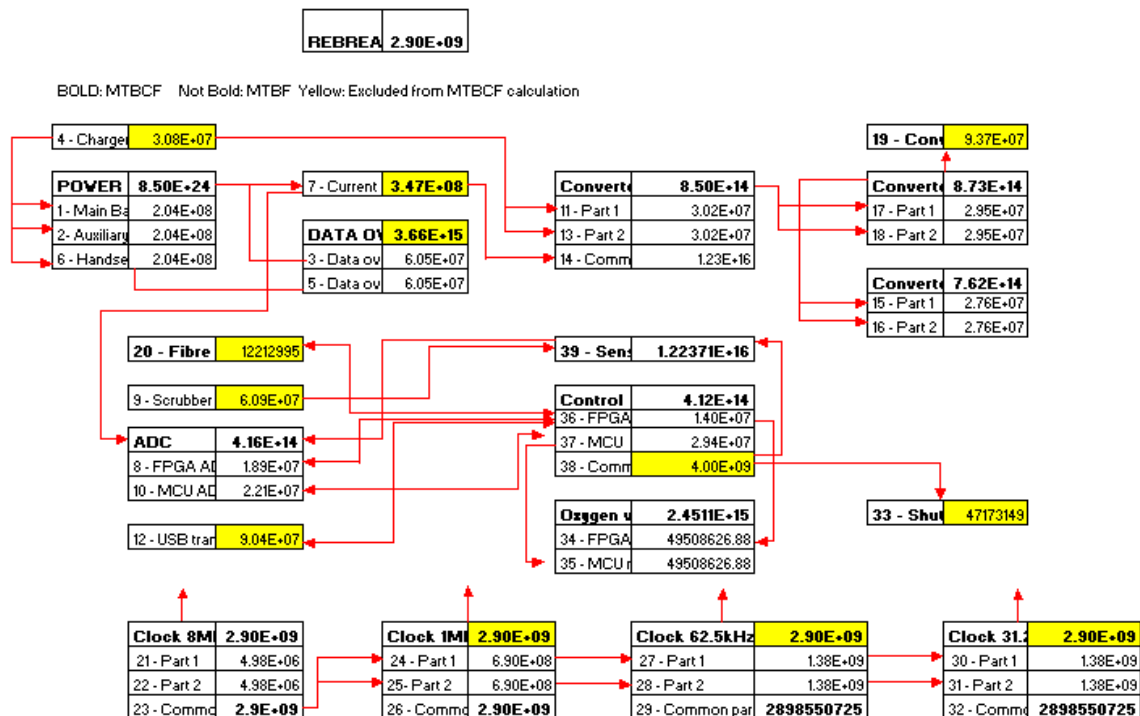

Figure 1: MTBF and MTBCF for each electronic block, and overall, for a single scrubber system