

DEEP LIFE OPEN REVOLUTION FAMILY OF REBREATHERS

Failure Mode, Effect and Criticality Analysis Volume 1: Root Document

DOCUMENT NUMBER:
[Filename] FMECA_OR_V1_Top_090529

ORIGINATOR: Review team comprising Dr. Alex Deas, Marat Yevtukhov, Alexei Bogatchov, Dr. Bob Davidov, Vladimir Komarov, Dr. Sergei Malyutin, Dr. Oleg Zagreblenny, Dr Alexander Kudriashov, Igor Abrosimov, Dr. Sergei Pyko.

DEPARTMENT: Engineering

LAST UPDATED: 29th May 2009

REVISION: C0

APPROVALS	
/AD/ Project Manager	29 th May 2009 Date
/VK/ Quality Officer	29 th May 2009 Date

Controlled Document if RED

Classified Document
DO NOT COPY.

Copyright © 2005, 2006, 2009 Deep Life Ltd. All rights reserved

Revision History

Revision	Date	Description
A	18 May 2005	Update to DL RB upon project moving from R&D to Engineering phase.
B and B1	18 th Nov 2005, 16 th Oct 2006	Checked for material covered by NDAs removed, and passed for publication. B1 Update of volume titles Oct 2006 and inclusion of Commercial SCR.
C0	29 th May 2009	Revisions to comply fully with IEC EN 61508:2004, following audit by SIRA Certification, with updates for OR_Umbilical, OR_Incursion and OR_Apocalypse_TypeIV models.

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	4
2	CLASSIFICATION	4
3	BENCHMARKS	5
3.1.1	Competitive Benchmark and Statutory Standards as Benchmarks	5
3.1.2	Primary Benchmark.....	6
4	REDUNDANCY REVIEW	6
4.1	Number of O2 Sensors Required.....	6
4.2	Number of other redundant systems required.....	7
4.3	Redundancy of Communication.....	7
5	SAFETY TRACEABILITY	9
6	EN 61508 AUDIT	33
7	CONCLUSION	33

1 PURPOSE AND SCOPE

This is the FMECA of Deep Life's first Open Revolution Submission.

For ease of update and use, the complete FMECA is divided into volumes, of which this document is Volume One. The FMECA is a key part of the safety case, along with user focus reviews, test and verification reports, accident studies, engineering reviews. This documentation is managed within a safety and product lifecycle management process designed to comply with IEC EN 61508:2004 for all aspects of the product: the end to end scope of IEC EN 61508 is applied to mechanics, pneumatics and ergonomics as well as the electrical, electronic and programmed systems.

The FMECA is one part of the safety case for the rebreather, along with the Colour Books provide a detailed design description of the project, the standards compliance data, field test data, and other documents as set down in Quality Procedure QP20.

The FMECA volumes are:

Volume 1: This document, stating the scope of the project, providing the top level architectural description of how failures are managed.

Volume 2: Electronics MTBF and MTBCF Calculation

Volume 3: Bottom Up Electronics Review FMECA

Volume 4: Bottom Up Mechanical FMECA

Volume 5: Bottom Up Software, Firmware and Operational FMECA

Volume 6: Top Down HAZID

Volume 7: Hierarchical Top Down Fault Tree Analysis

Volume 8: Communications from Rebreather

The purpose here is to provide an overview of the failure modes, effect, redundancy, fault tolerance and criticality for review purposes during the design process.

2 CLASSIFICATION

Safety Engineers distinguish different degrees of defective operation. A "fault" is deemed to occur when some piece of equipment does not operate as designed. A "failure" only occurs if person other than a repairman has to cope with the situation. A "critical" failure endangers one or more people, and catastrophic failures kill more than 6 people, or 100 people, depending on the industry.

Safety engineers also identify different modes of safe operation: A "probabilistically safe" system has no single point of failure, and enough redundant sensors, logic, processors, and effectors that it is very unlikely to cause harm. "Very unlikely" to a Safety Engineer means less than one human life lost or serious injury in a billion hours of operation.

An "inherently safe" system is a clever arrangement, usually mechanical, that cannot be made to cause harm - obviously the best arrangement, but this is not always possible. For example, "inherently safe" airplanes are not possible.

A "**fail-safe**" system is one that cannot cause harm when it fails.

A "**fault-tolerant**" system can continue to operate with faults, though its operation may be degraded in some fashion but which does not affect the safety of the user significantly.

These terms combine to describe the safety needed by systems: For example, most biomedical equipment is only "critical," and often another identical piece of equipment is nearby, so it can be merely "**probabilistically fail-safe**".

Train signals can cause "catastrophic" accidents (imagine chemical releases from tank-cars) and are usually "inherently safe".

Aircraft "failures" are "catastrophic" (at least for their passengers and crew,) so aircraft are usually "**probabilistically fault-tolerant**".

Without any safety features, nuclear reactors would have "catastrophic failures", so real nuclear reactors are required to be at least "probabilistically fail-safe", and some are "inherently fault-tolerant".

The appropriate level for a rebreather is probabilistically fail-safe, probabilistically fault tolerant to achieve probability of a critical failure less than one per billion hours. The latter requires a MTBF calculation for each component path, and the probability of failure must be better than one in a billion hours of operation. Where this is not the case, redundancy and fail safe subsystems must be introduced to achieve at least a billion hours Mean Time Between Critical Failure. The mode of the failure must also be determined, and means put in place to ensure that all failures are in a fail-safe state, or a state that does not immediately endanger the life of the user.

3 BENCHMARKS

The first issue to resolve is what level of performance must be met. This is normally set by existing companies and standards. In the case of rebreathers, this is not possible, for the reasons described below.

3.1.1 Competitive Benchmark and Statutory Standards as Benchmarks

Existing equipment from a market leader would normally be taken as the competitive benchmark. Some manufacturers are CE approved and appear to work closely with BSAC who had a large input to EN14143 standard. Much of EN14143 appears to be written around the APD Inspiration.

Unfortunately no existing equipment meets any Functional Safety standard. This statements covers a wide range of situations in the market: in extremis, electronically controlled rebreathers are designed and sold widely yet the designer had never had any engineering training whatsoever. No contemporary rebreather meets the competency requirements of IEC EN 61508:2004, as defined by the CASS Scheme for EN 61508 certification.

A long list of single point potentially fatal failures can be given of most contemporary rebreather products: existing equipment is clearly not fail safe, and none can tolerate a single worst case fault. This means that no existing rebreather can be classified as a Dependable System nor a Fault Tolerant System. All three factors, fail safe, dependable and fault tolerant, are normally fundamental requirements of any life critical system.

For these reasons no contemporary benchmark is used for the electronic and programmed systems that form part of the Open Revolution family of rebreathers. However, there is a body of expertise for the respiratory performance. Benchmarks for respiratory performance are taken from the APD Inspiration, APD Evolution, ISC Megalodon, Draeger Dolphin and CCRB Ouroboros rebreathers, as well as compliance with standards, regulations and guidelines that relate to respiratory and general performance. These standards are listed in the EC PPE Technical File for the products.

3.1.2 Primary Benchmark

The entire design of the OPEN REVOLUTION rebreather has set as its benchmark:

- Fail Safe for both electrical and mechanical systems.
- Fault tolerant, able to operate as a rebreather with two worst case faults of random faults.
- Dependable. This means it must monitor using redundant systems, every factor that affects the well being of the user. This requires total gas monitoring, with a means to remove failure modes caused by the user: forums suggest that users fail to bail out when this is indicated, and most deaths result from this.

For reasons of economy, a unit may be fitted with fewer components than is needed for the primary benchmark, in which case the system must meet the basic benchmark, which is simply better than 1 billion hours between critical failures of the system. This is done for reasons of cost in some cost sensitive applications. Examples of such cost reduction include:

1. Fitment of one pressure sensor only, instead of multiple ambient sensors. This is possible if the unit is not used for decompression diving, therefore pressure is not a critical factor.
2. Fitment of one O₂ injector only instead of two or four: the bail out device will still provide a degree of fault tolerance.
3. Fitment of one scrubber sensor into the scrubber than expires first, on the basis that when that scrubber has expired, the dive should already have been aborted.
4. Fitment of fewer oxygen sensors.

4 REDUNDANCY REVIEW

4.1 Number of O₂ Sensors Required

The only oxygen sensing technology known to be suitable for this application is galvanic oxygen cells. Other methods that have been considered include MEM paramagnetic sensors, Zirconia oxide sensors, Sol-gel sensors, high pressure unique species mass spectrometry. A very detailed study of galvanic sensors was conducted.

Experiments on galvanic oxygen sensors indicate they have a minimum life of 18 months at a PPO₂ of 0.2, and this degrades linearly with PPO₂ above this: for example, at a PPO₂ of 1.2, some sensors have a life of just three months.

In a worst case dive, that is one which lasts as long as the maximum scrubber life, 5 hours, with an average PPO₂ of 1.2, the chance of a failure is 1 in $(0.2/1.2)^{24} * 1.5 * 365/5$, which is around 1 in 438 per dive. The chance of two sensors failing at the same time would appear to be 438^2 , which is 191,844. If the failures of the sensor can be identified consistently, then three sensors are needed to meet SIL 3 requirements, for MTBCF and MTBF.

This problem is exacerbated by the fact that towards the end of their life, all sensors will fail within a month of each other. During this period the probability of two sensors failing during a three hour period is reduced to one in $((0.2/1.2)^{24} * 1.5 * 365/5/12)^2$, which is 1 in 1332 dives. This means it is essential that effective self test is applied at the start of every dive and during the dive, to confirm the sensors are working with the desired accuracy.

It is noted that to use three sensors, the system must not use voting logic but the ability to operate with one working sensor out of three, as described under the O₂ sensing scheme, including detecting accurately any sensor failure, regardless of the failure mode. The

Released for publication

probability of a critical failure in this case on a five hour dive with average PPO2 of 1.2 is: $(0.2/1.2) * (24 * 1.5 * 365 * 5/3) * (5/12) ^ 3$, or 35 billion hours. This assumes all failures are independent: this is not the case with galvanic sensors. Efforts are made to increase sensor diversity by using sensors from different batches, and where possible from different vendors. All Open Revolution rebreathers with oxygen sensing (OR_Umbilical, OR_Incursion and OR_Apocalypse_TypeIV iCCR), have provision in the hardware for sol-gel sensors by simply a firmware upgrade, when the sol-gel technology is available. This provides an additional degree of diversity that would enable the products to move from SIL 3 to SIL 4.

4.2 Number of other redundant systems required

All other components, except the O2 sensor and CO2 sensor, either do not lead to a critical failure, or have a life of more than 100,000 hours. In this case, triple redundancy with check sums on each data have been determined to tolerate 2 worst case faults whilst still meeting achieve the billion hour critical failure target at an electronic level.

It is noted that it is not within ALARP to provide flood protection for more than one breathing loop.

4.3 Redundancy of Communication

It is noted that all communications between subsystem in the design are dual redundant. In particular, an optical communication link and an electrical link is used, the latter being data over power. The use of two different forms of communication is correct, as a failure mode such as from EMI that affects one channel, will not affect the other channel. All data has CRC bits added, so any corruption on a data channel can be detected and the data source excluded.

Loss of all communication would result in the handset / PFD continuing to operate, and the base unit continuing to operate. The former would assume a fixed PPO2 of 1.0, depth correct to PPO2 of 0.7 at the surface, each solenoid would take over control and maintain PPO2 at 1.0, unless within 10m of the surface, whereupon it would scale to a PPO2 of 0.7.

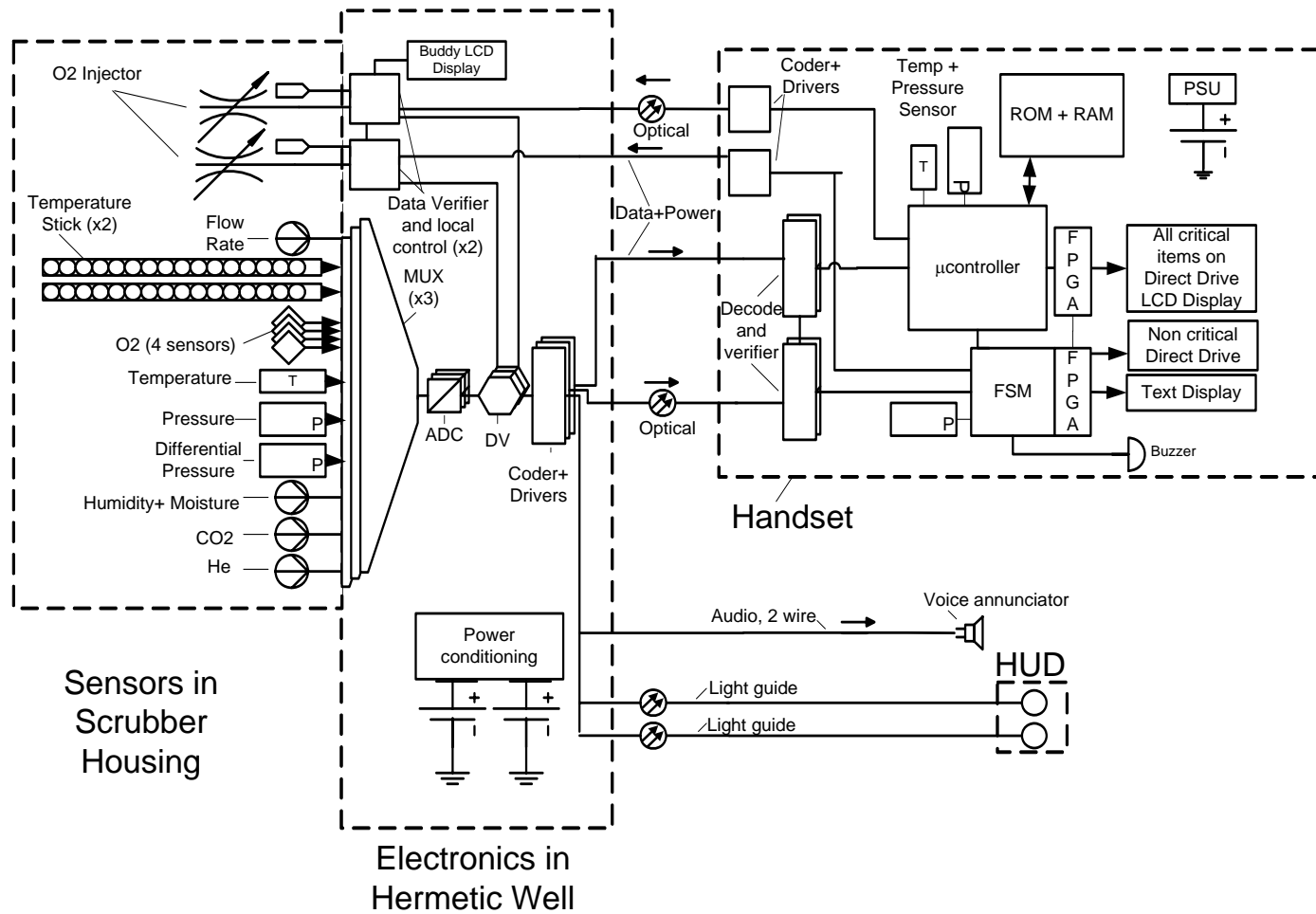


Figure 1: The fundamental electronic architecture of the Open Revolution family of products showing connectivity and major redundant and fault tolerant sections. Electronics in hermetic well is shown as a single board, where in practice it is two boards partitioned as described in the Project Green Book Specification at the outset. The Handset is implemented in the form of a PFD, and on the supervisor display. All displays are now AMOLED for greater visibility underwater than LCD. The Monitors on the Apocalypse implement this same architecture of diverse channels.

5 SAFETY TRACEABILITY

All safety requirements are maintained on a Mantis issue tracking system. Each issue has been reviewed for each of the following three models of the Open Revolution family of rebreathers:

- OR_Umbilical Commercial Diving Dual Scrubber eCCR / eSCR
- OR_Incursion Military Rebreather eCCR
- OR_Apocalypse_TypeIV Recreational iCCR

These are represented in the Compliance column of the table on the right as U, I and A respectively. The Minute of the review is recorded below.

MANTIS Hyperlink	Category	Summary Requirement (Refer to Mantis for detailed requirement)	Compliance		
			U	I	A
0000561	Oxygen Monitoring related Level	It shall be ensured O2 cells calibration calibration is not carried out in cells with water on their faces (FMECA V6 Risk 10.13)	Y	Y	Y
0000562	Oxygen Monitoring related Level	The training manual shall emphasise the checking of the unit by a Make-Up-Gas flush (FMECA V6 Risk 10.13)	Y	Y	Y
0000549	Oxygen Monitoring related Level	System shall withstand multiple O2 cell failures (FMECA V6 Risk 10.7, 10.8, 10.12, 10.13, 10.14)	Y	Y	Y
0000753	Oxygen Monitoring related Level	The flow of gas across the cell face shall be checked directly or indirectly during the dive (FMECA V6 Risk 10.13)	Y	Y	Y
0000752	Oxygen Monitoring related Level	Cells shall be positioned so water cannot drip onto their faces in any normal diver position (FMECA V6 Risk 10.13)	Y	Y	Y
0000751	Oxygen Monitoring related Level	Walls or rings around the membrane that can retain water in any orientation of the diver shall be avoided (FMECA V6 Risk 10.13)	Y	Y	Y
0000524	Controller Information related and	The main monitoring or control device shall have the largest display which it is practical to carry (FMECA V6 Risk 9.14)	Y	Y	Y
0000526	Controller Information related and	Alphanumeric displays shall be backlit (FMECA V6 Risk 9.14)	Y	Y	Y
0000743	Controller Information related and	If alphanumeric displays are used at all, they shall be supplemented by other annunciation devices (FMECA V6 Risk 9.14)	Y	Y	Y

0000742	Controller Information related	and	A vibrating device or a very bright LED close to the diver's mask shall be used (FMECA V6 Risk 9.11)	Y	Y	Y
0000741	Controller Information related	and	If voice annunciation is used, then the problem shall be announced and the action shall be emphasised (FMECA V6 Risk 9.11)	Y	Y	Y
0000740	Controller Information related	and	If an alphanumeric display is used then the failure and the action shall be displayed (FMECA V6 Risk 9.11)	Y	Y	Y
0000739	Controller Information related	and	If the diver is monitoring himself, then the actual monitoring rate shall itself be monitored (FMECA V6 Risk 9.11)	Y	Y	Y
0000738	Controller Information related	and	The primary information device shall not be a handset (FMECA V6 Risk 9.11)	Y	Y	Y
0000519	Controller Information related	and	Multiple annunciation shall be provided (FMECA V6 Risk 9.11)	Y	Y	Y
0000737	Umbilical-Supplied Dives related		User manual shall require diver to check one-way valve before every dive (FMECA V6 Risk 17.14)	Y	Y	Y
0000736	Controller Information related	and	The Functional Safety process or the Functional Safety of the design shall be audited (FMECA V6 Risk 9.12)	Y	Y	Y
0000735	Controller Information related	and	All staff working on software shall meet CASS Competency Levels (FMECA V6 Risk 9.12)	Y	Y	Y
0000521	Controller Information related	and	Normal practices for non-safety-related software, such as automated GUI checks, shall not be applied (FMECA V6 Risk 9.12)	Y	Y	Y
0000732	Diver Physiology related		Equivalent Air Depths (E.A.D) shall be monitored (FMECA V6 Risk 18.14, 18.15)	Y	Y	Y
0000734	Diver Physiology related		Narcosis hazard shall be stated clearly in training manuals of contributory factors (FMECA V6 Risk 18.14)	Y	Y	Y
0000733	Diver Physiology related		User manual shall warn clearly of Argon risks in oxygen (FMECA V6 Risk 18.14)	Y	Y	Y
0000727	Controller Information related	and	Three power sources shall be provided (FMECA V6 Risk 9.1, 9.2)	Y	Y	Y
0000576	Carbon Dioxide		Granular material packed by users shall not be	Y	Y	Y

	Level related	used (FMECA V6 Risk 11.4)			
0000712	Diver Physiology related	A Diver Emergency Switch for the commercial diver using a helmet shall be provided (FMECA V6 Risk 18.11)	Y	Y	Y
0000723	Safety related Process	A Safety certification body shall have a strong ethical and moral responsible (FMECA V6 Risk 20.3)	Y	Y	Y
0000725	Safety related Process	Rebreather's electronic or programmed part failure to meet Safety standard to be incompetence and negligence(FMECA V6 Risk 20.3)	Y	Y	Y
0000724	Safety related Process	Manufacturers shall have a responsibility to ensure the Safety certification body is fully informed (FMECA V6 Risk 20.3)	Y	Y	Y
0000722	Safety related Process	IEE/BCS grades shall be applied, increasing with increasing SIL level (FMECA V6 Risk 20.1)	Y	Y	Y
0000721	Safety related Process	FMECA shall be reviewed annualy (FMECA V6 Risk 20.1)	Y	Y	Y
0000720	Diver Physiology related	Counter-diffusion hazard shall be stated clearly in training manuals (FMECA V6 Risk 18.13)	Y	Y	Y
0000719	Diver Physiology related	N2 shall be measured with an alarm if less than 500mbar of N2 (FMECA V6 Risk 18.13)	Y	Y	Y
0000718	Diver Physiology related	Instruction and information on pulmonary exposure risks shall be provided (FMECA V6 Risk 18.12)	Y	Y	Y
0000717	Diver Physiology related	Respiratory parameters shall be measured (FMECA V6 Risk 18.11)	Y	Y	Y
0000716	Diver Physiology related	WOB shall be measured actively pre-dive and during the dive (FMECA V6 Risk 18.11)	Y	Y	Y
0000715	Diver Physiology related	EAC scrubber shall be used (FMECA V6 Risk 18.11)	Y	Y	Y
0000714	Diver Physiology related	All scrimms shall be eliminated in the design (FMECA V6 Risk 18.11)	Y	Y	Y
0000713	Diver Physiology related	There shall be no measurable loss of lung surficant during a dive (FMECA V6 Risk 18.11)	Y	Y	Y
0000711	Diver Physiology related	CCR controller shall track CNS and maintain within safe limit (FMECA V6 Risk 18.11)	Y	Y	Y
0000710	Diver Physiology related	Modified CNS algorithm, with margin to reduce statistical incidence of measurable CNS	Y	Y	Y

		damage shall be used (FMECA V6 Risk 18.11)			
0000709	Diver Physiology related	Divers shall be advised that below 7C, gas heating is required, and particularly below 4C (FMECA V6 Risk 18.10)	Y	Y	Y
0000708	Diver Physiology related	The lowest practicable Work of Breathing shall be achieved (FMECA V6 Risk 18.9)	Y	Y	Y
0000707	Diver Physiology related	Deco algorithm shall be verified to be implemented correctly using formal methods (FMECA V6 Risk 18.8)	Y	Y	Y
0000706	Diver Physiology related	O2 Cells shall be calibrated in air when the unit is open (FMECA V6 Risk 18.7)	Y	Y	Y
0000705	Diver Physiology related	The number of fingers in the web around the mushroom valve shall be kept to the minimum (FMECA V6 Risk 18.6)	Y	Y	Y
0000704	Diver Physiology related	Breathing hose shall be of sufficient diameter so as not to be blocked by vomit (FMECA V6 Risk 18.6)	Y	Y	Y
0000703	Diver Physiology related	A combined ALV/BOV shall be always in the loop (FMECA V6 Risk 18.6)	Y	Y	Y
0000702	Diver Physiology related	All materials shall be checked for off-gassing both from the MSDS and from rigorous materials testing (FMECA V6 Risk 18.5)	Y	Y	Y
0000701	Diver Physiology related	All allergenic materials shall be eliminated from loop (FMECA V6 Risk 18.5)	Y	Y	Y
0000700	Diver Physiology related	2kPa scrubber endurance ratings shall be provided (FMECA V6 Risk 18.3)	Y	Y	Y
0000699	Diver Physiology related	Scrubber shall have uniform endurance with depth and temperature, with the application of ALARP (FMECA V6 Risk 18.3)	Y	Y	Y
0000692	Umbilical-Supplied Dives related	A fail-safe automatic shut off valve shall be implemented (FMECA V6 Risk 18.1, 18.4)	Y	Y	Y
0000698	Diver Physiology related	WOB shall be minimised with the application of ALARP (FMECA V6 Risk 18.3)	Y	Y	Y
0000697	Diver Physiology related	Scrubber health shall be monitored with the application of ALARP (FMECA V6 Risk 18.3)	Y	Y	Y
0000696	Diver Physiology related	Scrubber life shall be monitored with the application of ALARP (FMECA V6 Risk 18.3)	Y	Y	Y
0000695	Diver Physiology related	Exhaled CO2 shall be monitored to monitor retained CO2 (FMECA V6 Risk 18.3)	Y	Y	Y

0000694	Diver Physiology related	Diver's CNS and Pulmonary O2 exposure shall be tracked (FMECA V6 Risk 18.2)	Y	Y	Y
0000693	Diver Physiology related	PPO2 shall be controlled (FMECA V6 Risk 18.2)	Y	Y	Y
0000691	Diver Physiology related	Functional Safety life-cycle process appropriate to SIL assessment shall be applied (FMECA V6 Risk 18.1)	Y	Y	Y
0000690	Umbilical-Supplied related Dives	ALVBOV shall be used (FMECA V6 Risk 17.15)	Y	Y	Y
0000689	Umbilical-Supplied related Dives	The operation of the one-way valves shall be a pre-dive check (FMECA V6 Risk 17.15)	Y	Y	Y
0000688	Umbilical-Supplied related Dives	The one-way valve shall be properly characterised (FMECA V6 Risk 17.15)	Y	Y	Y
0000687	Umbilical-Supplied related Dives	Two one-way valves in series shall be used (FMECA V6 Risk 17.15)	Y	Y	Y
0000686	Umbilical-Supplied related Dives	Liquid crystal electrolytic materials for the electronics shell shall be considered for use (FMECA V6 Risk 17.13)	Y	Y	Y
0000685	Umbilical-Supplied related Dives	Internal electronics shall be shielded for magnetically induced currents (FMECA V6 Risk 17.13)	Y	Y	Y
0000684	Umbilical-Supplied related Dives	The highest possible current density with the unit in water to be used during testing (FMECA V6 Risk 17.13)	Y	Y	Y
0000683	Umbilical-Supplied related Dives	Equipment shall be tested for operation between a pair of underwater burning system electrodes in use (FMECA V6 Risk 17.13)	Y	Y	Y
0000682	Umbilical-Supplied related Dives	Active current monitoring shall be used to detect shorts or excess current drain (FMECA V6 Risk 17.12)	Y	Y	Y
0000681	Umbilical-Supplied related Dives	Failure mode to be eliminated by use of self-regulating materials (FMECA V6 Risk 17.12)	Y	Y	Y
0000680	Umbilical-Supplied related Dives	Gas heating shall be treated as a SIL-4 requirement for very deep diving (FMECA V6 Risk 17.11)	Y	Y	Y
0000679	Umbilical-	A requirement shall be stated for passive	Y	Y	Y

	Supplied related	Dives	undersuit thermal protection in user manuals and training (FMECA V6 Risk 17.11)			
0000678	Umbilical-Supplied related	Dives	Special considerations to be used in warm water conditions (FMECA V6 Risk 17.10)	Y	Y	Y
0000677	Umbilical-Supplied related	Dives	Full safety case is required for diver thermal balance (FMECA V6 Risk 17.10)	Y	Y	Y
0000676	Umbilical-Supplied related	Dives	A dry suit shall be used with a rebreather (FMECA V6 Risk 17.9)	Y	Y	Y
0000675	Umbilical-Supplied related	Dives	Breathing gas heating shall be heated (FMECA V6 Risk 17.9)	Y	Y	Y
0000674	Umbilical-Supplied related	Dives	Communication to bell shall be provided (FMECA V6 Risk 17.8)	Y	Y	Y
0000673	Umbilical-Supplied related	Dives	Two communication paths to be used (FMECA V6 Risk 17.8)	Y	Y	Y
0000669	Umbilical-Supplied related	Dives	Strict control of breathing gas, and RoHS compliant components in the dive system shall be provided (FMECA V6 Risk 17.7)	Y	Y	Y
0000668	Umbilical-Supplied related	Dives	Active HC and VOC monitoring on the diver shall be provided (FMECA V6 Risk 17.7)	Y	Y	Y
0000667	Umbilical-Supplied related	Dives	Diver training shall cover awareness of the symptoms of CO (FMECA V6 Risk 17.6)	Y	Y	Y
0000666	Umbilical-Supplied related	Dives	Active CO monitoring on the diver for very long dives shall be provided (FMECA V6 Risk 17.6)	Y	Y	Y
0000665	Umbilical-Supplied related	Dives	Use only certified diving gas shall be explicit in the user manual (FMECA V6 Risk 17.6)	Y	Y	Y
0000664	Umbilical-Supplied related	Dives	Diver shall be trained to descend slow enough for the SCR to fill loop (FMECA V6 Risk 17.5)	Y	Y	Y
0000663	Associated Equipment related		Every fault against every unit from the RB history shall be checked, to ensure it is not repeated (FMECA V6 Risk 14.3)	Y	Y	Y
0000662	Umbilical-		The system shall have an underpressure valve	Y	Y	Y

	Supplied related	Dives	on the helmet, and this shall allow flooding of the suit (FMECA V6 Risk 17.5)			
0000657	Umbilical-Supplied related	Dives	Adequate bail-out is required (FMECA V6 Risk 17.2, 17.5)	Y	Y	Y
0000656	Umbilical-Supplied related	Dives	One-way valve is required (FMECA V6 Risk 17.2, 17.5)	Y	Y	Y
0000661	Umbilical-Supplied related	Dives	Whether a helmet is attached correctly shall be monitored electronically (FMECA V6 Risk 17.4)	Y	Y	Y
0000660	Umbilical-Supplied related	Dives	Weight of umbilical shall be controlled (FMECA V6 Risk 17.3)	Y	Y	Y
0000659	Umbilical-Supplied related	Dives	Procedures to avoid diver entrapment shall be used (FMECA V6 Risk 17.3)	Y	Y	Y
0000658	Umbilical-Supplied related	Dives	Umbilical shall be either disconnectable or diver shall carry means to cut the umbilical to free himself (FMECA V6 Risk 17.3)	Y	Y	Y
0000655	Umbilical-Supplied related	Dives	Protection to avoid reduction in diameter from increasing risk of it being severed shall be considered (FMECA V6 Risk 17.1)	Y	Y	Y
0000654	Umbilical-Supplied related	Dives	A transponder separated to the rebreather shall be put onto the diver (FMECA V6 Risk 17.1)	Y	Y	Y
0000653	Umbilical-Supplied related	Dives	Bail-out carried by diver shall be used in case of loss umbilical (FMECA V6 Risk 17.1)	Y	Y	Y
0000652	Dives in Cold Water related		Divers shall be advised that below 7C, gas heating is required, and particularly below 4C (FMECA V6 Risk 16.2)	Y	Y	Y
0000651	Dives in Cold Water related		Equipment to be tested with storage to minus 30C, for material suitability (FMECA V6 Risk 16.1)	Y	Y	Y
0000650	Dives in Cold Water related		Equipment shall be stored in a warm location (FMECA V6 Risk 16.1)	Y	Y	Y
0000649	Dives in Cold Water related		SIL rated heating system in the counterlungs shall be used for diving in very cold water (FMECA V6 Risk 16.1)	Y	Y	Y
0000648	Associated Equipment		Hooks and lines that increase the entrapment risk significantly shall be avoided (FMECA V6	Y	Y	Y

	realted	Risk 14.2)			
0000647	Associated Equipment realted	Active suit heating using self-regulating carbon monomers shall be provided (FMECA V6 Risk 14.1)	Y	Y	Y
0000646	Associated Equipment realted	Dry gloves that allow entire suit to flood shall not be used for decompression diving without suit heating (FMECA V6 Risk 14.1)	Y	Y	Y
0000645	Other Rebreather Equipment related	Divers shall be trained not to fix rebreather to their body except using harness that came with rebreather (FMECA V6 Risk 13.6)	Y	Y	Y
0000644	Other Rebreather Equipment related	Hooks and lines that increase the entrapment risk significantly shall be avoided (FMECA V6 Risk 13.6)	Y	Y	Y
0000643	Other Rebreather Equipment related	Silicone shall be used for seals that are not in contact with high pressure oxygen (FMECA V6 Risk 13.5)	Y	Y	Y
0000642	Other Rebreather Equipment related	PTFE to be used for high pressure valve seat material and high pressure oxygen hose liners(FMECA V6 Risk 13.5)	Y	Y	Y
0000641	Other Rebreather Equipment related	Fully reacted Thermoplastic PUs formed from polyether polyols to be used for strong and flexible parts (FMECA V6 Risk 13.5)	Y	Y	Y
0000640	Other Rebreather Equipment related	TPEE polyester free of plasticizers and softeners shall not be used for high pressure gas (FMECA V6 Risk 13.5)	Y	Y	Y
0000639	Other Rebreather Equipment related	TPEE polyester free of plasticizers and softeners to be used for medium pressure hose core material (FMECA V6 Risk 13.5)	Y	Y	Y
0000638	Other Rebreather Equipment related	Natural rubber and latex shall not be used due to prevalence of an allergenic response to these materials (FMECA V6 Risk 13.5)	Y	Y	Y
0000637	Other Rebreather Equipment related	PVC and Ethyl PU shall not be used (FMECA V6 Risk 13.5)	Y	Y	Y
0000636	Other Rebreather Equipment related	The number of different plastics used shall be kept to the absolute minimum (FMECA V6 Risk 13.5)	Y	Y	Y
0000635	Other Rebreather Equipment related	The failure modes of the pressure sensors shall be determined, and failure actively detected (FMECA V6 Risk 13.4)	Y	Y	Y
0000634	Other Rebreather Equipment	Multiple attachment points for the harness shall be used (FMECA V6 Risk 13.3)	Y	Y	Y

	related				
0000633	Other Rebreather Equipment related	BC to be sold with rebreather, where a BC will be used (FMECA V6 Risk 13.2)	Y	Y	Y
0000632	Other Rebreather Equipment related	The test systems shall be designed to subject the equipment to twice the maximum operating depth (FMECA V6 Risk 13.1)	Y	Y	Y
0000631	Other Rebreather Equipment related	It shall be ensure equipment is designed and verified to operate to at twice the maximum operating depth (FMECA V6 Risk 13.1)	Y	Y	Y
0000630	Flooding or Drowning related	OPV to be vented at a sufficient rate for the worst case ascent (FMECA V6 Risk 12.5)	Y	Y	Y
0000627	Flooding or Drowning related	It shall be ensured rebreather can withstand underpressure or overpressure by one bar (FMECA V6 Risk 12.5)	Y	Y	Y
0000629	Flooding or Drowning related	The effect of compressing a rebreather all ports closed and gas off shall be assest, to the maximum depth (FMECA V6 Risk 12.5)	Y	Y	Y
0000628	Flooding or Drowning related	It shall be ensure rebreather can withstand a total pressure of double the maximum diving depth (FMECA V6 Risk 12.5)	Y	Y	Y
0000626	Flooding or Drowning related	A reinforcing ring to the counterlung that positively latches the port mouldings shall be fitted (FMECA V6 Risk 12.4)	Y	Y	Y
0000625	Flooding or Drowning related	It shall be ensured ports and counterlungs withstand a 100kg pull (FMECA V6 Risk 12.4)	Y	Y	Y
0000623	Flooding or Drowning related	It shall be ensure the mouthpiece can withstand the weight of a diver (100kg for 1 minute) (FMECA V6 Risk 12.3)	Y	Y	Y
0000622	Flooding or Drowning related	A mouthpiece retainer shall be fitted as standard (FMECA V6 Risk 12.2, 12.3)	Y	Y	Y
0000624	Flooding or Drowning related	It shall be ensure all hoses and connectors can withstand the weight of a diver (100kg for 1 minute) (FMECA V6 Risk 12.3)	Y	Y	Y
0000606	Flooding or Drowning related	The breathing loop shall shut automatically if the mouthpiece is not in the diver's mouth (FMECA V6 Risk 12.1, 12.2)	Y	Y	Y
0000621	Flooding or Drowning related	It shall be ensured the BC is big enough to lift a flooded rebreather (FMECA V6 Risk 12.2)	Y	Y	Y
0000620	Flooding or Drowning related	Double seals shall be used to minimise the leak risk where within ALARP (FMECA V6 Risk	Y	Y	Y

		12.1)			
0000619	Flooding or Drowning related	Connectors to be secure and not detach accidentally (FMECA V6 Risk 12.1)	Y	Y	Y
0000618	Flooding or Drowning related	Double layer Counterlungs shall be avoided (FMECA V6 Risk 12.1)	Y	Y	Y
0000617	Flooding or Drowning related	Lip seals shall be used for protected moving surfaces (FMECA V6 Risk 12.1)	Y	Y	Y
0000616	Flooding or Drowning related	Seals around scrubber shall stand over-pressure and under-pressure (FMECA V6 Risk 12.1)	Y	Y	Y
0000615	Flooding or Drowning related	Counterlung fittings require a welded retainer ring to prevent them pulling out of the counterlung (FMECA V6 Risk 12.1)	Y	Y	Y
0000614	Flooding or Drowning related	It shall be ensure ALV diaphragm does not fold, and is tear resistant (FMECA V6 Risk 12.1)	Y	Y	Y
0000613	Flooding or Drowning related	It shall be ensure OPV diaphragm does not fold, and is tear resistant (FMECA V6 Risk 12.1)	Y	Y	Y
0000612	Flooding or Drowning related	Full hose connector as an integral part of the scrubber canister shall be provided (FMECA V6 Risk 12.1)	Y	Y	Y
0000611	Flooding or Drowning related	Hoses shall be made from EPDM (FMECA V6 Risk 12.1)	Y	Y	Y
0000610	Flooding or Drowning related	It shall be ensure counterlung can withstand shock pressures of 500mbar (FMECA V6 Risk 12.1)	Y	Y	Y
0000609	Flooding or Drowning related	Positive identification and colouring shall be used for the connectors (FMECA V6 Risk 12.1)	Y	Y	Y
0000608	Flooding or Drowning related	Moisture and WOB shall be monitored (FMECA V6 Risk 12.1)	Y	Y	Y
0000607	Flooding or Drowning related	A buoyancy device shall be fitted to SCUBA rebreathers with enough lift for the diver (FMECA V6 Risk 12.1)	Y	Y	Y
0000605	Flooding or Drowning related	A mouthpiece retainer (gag strap) as standard shall be fitted (FMECA V6 Risk 12.1)	Y	Y	Y
0000604	Carbon Dioxide Level related	Loop operation under all plausible fault conditions and pressures using formal methods shall be verified (FMECA V6 Risk 11.1)	Y	Y	Y
0000603	Carbon Dioxide	Any structure that can bypass the scrubber	Y	Y	Y

	Level related	under any circumstances shall not be used (FMECA V6 Risk 11.14)			
0000602	Carbon Dioxide Level related	WOB shall be verified not to increase suddenly with negative loop pressures (FMECA V6 Risk 11.13)	Y	Y	Y
0000601	Carbon Dioxide Level related	Counterlung material performance shall be verified under a wider range of conditions (FMECA V6 Risk 11.12)	Y	Y	Y
0000600	Carbon Dioxide Level related	Effect of reversed flow shall be assessed (FMECA V6 Risk 11.11)	Y	Y	Y
0000599	Carbon Dioxide Level related	Connectors and hose lengths shall be designed so it is not possible to swap the hoses accidentally (FMECA V6 Risk 11.11)	Y	Y	Y
0000598	Carbon Dioxide Level related	One-way valve assemblies shall be designed so it is impossible to swap webs from inhale to exhale (FMECA V6 Risk 11.11)	Y	Y	Y
0000597	Carbon Dioxide Level related	One-way valve assembly shall be designed so it is impossible to insert mushrooms from wrong side of web (FMECA V6 Risk 11.11)	Y	Y	Y
0000596	Carbon Dioxide Level related	Hoses shall not kink or pinch (FMECA V6 Risk 11.10)	Y	Y	Y
0000595	Carbon Dioxide Level related	Audible warning of flood shall be provided (FMECA V6 Risk 11.9)	Y	Y	Y
0000594	Carbon Dioxide Level related	Electronic flood warnings where within ALARP to do so shall be provided (FMECA V6 Risk 11.9)	Y	Y	Y
0000593	Carbon Dioxide Level related	Water traps in mouthpiece as well as in counterlungs shall be provided (FMECA V6 Risk 11.9)	Y	Y	Y
0000592	Carbon Dioxide Level related	User manual shall explain caustic risk and avoid diver having scrubber liquid touch lips, face, or tongue(FMECA V6 Risk 11.9)	Y	Y	Y
0000591	Carbon Dioxide Level related	EACs to minimise risk of caustic cocktail shall be used (FMECA V6 Risk 11.9)	Y	Y	Y
0000590	Carbon Dioxide Level related	The rebreather shall be highly resistant to flooding, using double seals where reasonable possible (FMECA V6 Risk 11.9)	Y	Y	Y
0000589	Carbon Dioxide Level related	The flapper valve shall not seal shut if one small area is frozen (FMECA V6 Risk 11.8)	Y	Y	Y
0000588	Carbon Dioxide Level related	Water shall not collect around the flapper valve (FMECA V6 Risk 11.8)	Y	Y	Y

0000587	Carbon Dioxide Level related	The holes in the web shall be of sufficient size to let small particulate through and not jam (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000586	Carbon Dioxide Level related	The web shall be tested to ensure the mushroom cannot fold into the web regardless of shock (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000585	Carbon Dioxide Level related	The valve shall preferably be designed to make a soft click sound each time it closes (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000584	Carbon Dioxide Level related	Two webs shall be different size, or keyed, to prevent inhale valve being inserted in exhale valve (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000583	Carbon Dioxide Level related	The web supporting the mushroom shall have means to prevent it being assembled on wrong side of web (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000582	Carbon Dioxide Level related	The flapper valve assembly shall be colour-coded (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000581	Carbon Dioxide Level related	One-way valve, Flapper valve design shall be of a type that shall not stick by itself (FMECA V6 Risk 11.7, 11.8)	Y	Y	Y
0000580	Carbon Dioxide Level related	Active monitoring of respiratory parameters shall be provided (FMECA V6 Risk 11.6)	Y	Y	Y
0000579	Carbon Dioxide Level related	Counterlungs shall be fixed down so that user cannot disconnect one end, or fail to attach counterlungs (FMECA V6 Risk 11.6)	Y	Y	Y
0000578	Carbon Dioxide Level related	WOB shall be measured actively during dive (FMECA V6 Risk 11.5)	Y	Y	Y
0000577	Carbon Dioxide Level related	EAC shall be used (FMECA V6 Risk 11.4)	Y	Y	Y
0000570	Carbon Dioxide Level related	Scrubber health shall be monitored (FMECA V6 Risk 11.1, 11.2, 11.3, 11.4)	Y	Y	Y
0000572	Carbon Dioxide Level related	It shall be monitored when the scrubber is changed (FMECA V6 Risk 11.1, 11.3, 11.4)	Y	Y	Y
0000571	Carbon Dioxide Level related	Scrubber life shall be monitored (FMECA V6 Risk 11.1, 11.3, 11.4)	Y	Y	Y
0000573	Carbon Dioxide Level related	PPCO2 shall be monitored (FMECA V6 Risk 11.1, 11.3, 11.4)	Y	Y	Y
0000575	Carbon Dioxide Level related	Monitoring of expired CO2 in iCCR and eCCRs/ eSCRs shall be provided (FMECA V6 Risk 10.12)	Y	Y	Y

0000574	Carbon Dioxide Level related	It shall be ensured scrubber seals can tolerate a large degree of scrubber damage (FMECA V6 Risk 11.2)	Y	Y	Y
0000569	Oxygen Monitoring Level related	Hypoxia risk alarm that does not use oxygen sensors shall be used (FMECA V6 Risk 10.18)	Y	Y	Y
0000568	Oxygen Monitoring Level related	It shall be ensure manuals state risk caustic burn from leaking electrolyte clearly and action to be taken (FMECA V6 Risk 10.17)	Y	Y	Y
0000567	Oxygen Monitoring Level related	Very thorough O2 cell screening shall be used (FMECA V6 Risk 10.16)	Y	Y	Y
0000566	Oxygen Monitoring Level related	O2 sensors shall be verified to ensure there is no electrolyte leakage if dropped (FMECA V6 Risk 10.15)	Y	Y	Y
0000565	Oxygen Monitoring Level related	Operators shall be warned to wash the sensor and hands in warm water immediately if an O2 Cell feels wet (FMECA V6 Risk 10.15)	Y	Y	Y
0000564	Oxygen Monitoring Level related	It shall be verified that O2 sensors specified not produce shrapnel when suddenly decompressed (Torpedo test) (FMECA V6 10.15)	Y	Y	Y
0000563	Oxygen Monitoring Level related	It shall be ensured the design allows adequate gas flow to rear of cells (FMECA V6 Risk 10.14)	Y	Y	Y
0000550	Oxygen Monitoring Level related	The O2 cells shall be engineered so all failures are in the same direction (FMECA V6 Risk 10.7, 10.8, 10.12, 10.14)	Y	Y	Y
0000560	Oxygen Monitoring Level related	O2 sensors shall be calibrated on air (FMECA V6 Risk 10.11)	Y	Y	Y
0000555	Oxygen Monitoring Level related	Means to check sensors automatically when a sensor failure occurs shall be provided (FMECA V6 Risk 10.9, 10.10)	Y	Y	Y
0000559	Oxygen Monitoring Level related	Different colour sensor bodies for each year shall be used (FMECA V6 Risk 10.10)	Y	Y	Y
0000558	Oxygen Monitoring Level related	O2 sensors shall be marked very clearly in large letters with a date code (FMECA V6 Risk 10.10)	Y	Y	Y
0000557	Oxygen Monitoring Level related	Pre-dive checks shall force the checking of the O2 sensors (FMECA V6 Risk 10.10)	Y	Y	Y

	related					
0000556	Oxygen Monitoring related	Level	Visual feedback in PFD in addition to audible alarms, or vibrating mouthpiece shall be used (FMECA V6 Risk 10.10)	Y	Y	Y
0000553	Oxygen Monitoring related	Level	O2 sensor fusion algorithm shall be used that can detect one good sensor among faulty sensors (FMECA V6 Risk 10.9, 10.10)	Y	Y	Y
0000554	Oxygen Monitoring related	Level	A fault assessment of O2 Cell failure modes shall be carried out (FMECA V6 Risk 10.9)	Y	Y	Y
0000552	Oxygen Monitoring related	Level	O2 cells shall be loaded to produce the lowest output voltage consistent with achieving the desired SNR (FMECA V6 Risk 10.8)	Y	Y	Y
0000551	Oxygen Monitoring related	Level	O2 sensor ceiling shall be tested by injecting a charge into the sensor to simulate PPO2 of 2.5 atm (FMECA V6 Risk 10.8)	Y	Y	Y
0000548	Oxygen Monitoring related	Level	SMB connector shall be used to minimise risk (FMECA V6 Risk 10.6)	Y	Y	Y
0000541	Oxygen Monitoring related	Level	The electronics shall check that the correct O2 sensor type is fitted and the fixed load is present (FMECA V6 Risk 10.1, 10.5)	Y	Y	Y
0000540	Oxygen Monitoring related	Level	The temperature compensation circuit shall be removed from O2 sensor and replaced with a fixed load (FMECA V6 Risk 10.1, 10.5)	Y	Y	Y
0000547	Oxygen Monitoring related	Level	System shall check for O2 sensor drift during successive calibration cycles (FMECA V6 Risk 10.4)	Y	Y	Y
0000546	Oxygen Monitoring related	Level	System shall check for need for O2 sensor replacement (FMECA V6 Risk 10.4)	Y	Y	Y
0000545	Oxygen Monitoring related	Level	All O2 sensors shall not be wired to one chip , whether one ADC, one MUX or one op-amp block (FMECA V6 Risk 10.3)	Y	Y	Y
0000544	Oxygen Monitoring related	Level	A connector which mates ground before signal, and protects the connections from corrosion shall be used (FMECA V6 Risk 10.3)	Y	Y	Y
0000542	Oxygen Monitoring related	Level	O2 flush under start-up sequence control shall be done to detect O2 sensors have CO2 contamination (FMECA V6 Risk 10.2)	Y	Y	Y
0000539	Controller Information	and	Bail out valve to be produced from durable materials (FMECA V6 Risk 9.23)	Y	Y	Y

	related					
0000538	Controller Information related	and	It shall be ensured diver can reach tank valves in SCUBA applications (FMECA V6 Risk 9.23)	Y	Y	Y
0000537	Controller Information related	and	Separate annunciation shall be provided as well as bail out actuator(FMECA V6 Risk 9.23)	Y	Y	Y
0000536	Controller Information related	and	Actuator shall be protected from user tampering (FMECA V6 Risk 9.23)	Y	Y	Y
0000535	Controller Information related	and	Actuator shall be achieved with just one moving part (FMECA V6 Risk 9.23)	Y	Y	Y
0000534	Controller Information related	and	All electronics and programmed parts of the rebreather shall comply with functional safety standards (FMECA V6 Risk 9.21)	Y	Y	Y
0000533	Controller Information related	and	MTBCF shall be calculated for entire electronics system (FMECA V6 Risk 9.21)	Y	Y	Y
0000509	Controller Information related	and	It shall be ensured unit powers on automatically whenever the PPO2 is less than 0.16 (FMECA V6 Risk 9.8, 9.20)	Y	Y	Y
0000532	Controller Information related	and	Failure modes due to cycling of brown-out events shall be verified (FMECA V6 Risk 9.19)	Y	Y	Y
0000531	Controller Information related	and	High degree of data line protection is required (FMECA V6 Risk 6.18)	Y	Y	Y
0000530	Controller Information related	and	Interrupts shall be avoided (FMECA V6 Risk 9.17)	Y	Y	Y
0000529	Controller Information related	and	Effect of watchdog and brown out circuits firing repeatedly and blocking other actions shall be considered (FMECA V6 Risk 9.17)	Y	Y	Y
0000527	Controller Information related	and	Electronics, particularly monitoring or control devices shall be Functional Safety compliant (FMECA V6 Risk 9.15, 9.17)	Y	Y	Y
0000528	Controller Information related	and	When monitoring or control device has two sets, then a failure of one shall not cause failure of the whole (FMECA V6 Risk 9.15)	Y	Y	Y
0000525	Controller Information	and	Suitable materials to be chosen to minimise risk of displays damaged due to being dropped	Y	Y	Y

	related	and	or mishandled (FMECA V6 Risk 9.14)			
0000523	Controller Information related	and	Software to be fail safe, including a code CRC check as part of startup sequence (FMECA V6 Risk 9.13).	Y	Y	Y
0000522	Controller Information related	and	Software shall be formally verified (FMECA V6 Risk 9.12)	Y	Y	Y
0000520	Controller Information related	and	An automatic bail-out valve shall be provided (FMECA V6 Risk 9.11)	Y	Y	Y
0000518	Controller Information related	and	Components liable to explode shall be moved to to a 1 ATM environment outside the rebreather (FMECA V6 Risk 9.10)	Y	Y	Y
0000517	Controller Information related	and	All components liable to explode shall be eliminated (FMECA V6 Risk 9.10)	Y	Y	Y
0000516	Controller Information related	and	All components liable to offgas shall be removed from the the oil-filled volume (FMECA V6 Risk 9.9)	Y	Y	Y
0000515	Controller Information related	and	Food grade silicone oil shall be used to avoid a health hazard (FMECA V6 Risk 9.9)	Y	Y	Y
0000514	Controller Information related	and	Waxes (solid paraffins) shall not be used (FMECA V6 Risk 9.9)	Y	Y	Y
0000513	Controller Information related	and	Hydrocarbon filling oils shall not be used (FMECA V6 Risk 9.9)	Y	Y	Y
0000512	Controller Information related	and	Monitoring or control shall provide device switches on automatically when unit is used (FMECA V6 Risk 9.8)	Y	Y	Y
0000511	Controller Information related	and	PFD shall be provided which also switches on automatically and cannot switch off when unit is operational (FMECA V6 Risk 9.8)	Y	Y	Y
0000510	Controller Information related	and	All possibility that the unit can “hang” (FMECA V6 Risk 9.8)	Y	Y	Y
0000508	Controller Information related	and	The circuit shall have multiple clocks, power supplies and other circuits (FMECA V6 Risk 9.7)	Y	Y	Y
0000507	Controller Information	and	Any device hang failure shall be logged and the unit permanently locked out on the surface	Y	Y	Y

	related		(FMECA V6 Risk 9.7)			
0000506	Controller Information related	and	The start-up sequence should detect if an abnormal shutdown occurs (FMECA V6 Risk 9.7)	Y	Y	Y
0000505	Controller Information related	and	Routines shall apply predicates in input data (FMECA V6 Risk 9.7)	Y	Y	Y
0000504	Controller Information related	and	All unused memory locations shall be filled with recovery code (FMECA V6 Risk 9.7)	Y	Y	Y
0000503	Controller Information related	and	It shall be ensured state machines have redundant states to detect failure and return unit to safe operation (FMECA V6 Risk 9.7)	Y	Y	Y
0000502	Controller Information related	and	It shall be ensured Brown-Out circuit is operating by power cycle test (FMECA V6 Risk 9.7)	Y	Y	Y
0000501	Controller Information related	and	It shall be ensured Watchdog circuit is operating by halting the clock for the Watchdog period (FMECA V6 Risk 9.7)	Y	Y	Y
0000500	Controller Information related	and	All electronics and software shall meet EN 61508:2004 Parts 1 to 3 to at least SIL 2 (FMECA V6 Risk 9.6)	Y	Y	Y
0000499	Controller Information related	and	Base unit shall be made to at least automotive SQA 9002 standards and controls (FMECA V6 Risk 9.6)	Y	Y	Y
0000498	Controller Information related	and	PFD in addition to monitoring or control device to be provided (FMECA V6 Risk 9.6)	Y	Y	Y
0000497	Controller Information related	and	Multiple devices shall be used in monitoring or control device (FMECA V6 Risk 9.6)	Y	Y	Y
0000496	Controller Information related	and	Full electrical self-test testing to be performed during power-up sequence (FMECA V6 Risk 9.6, 9.10, 9.15, 9.16)	Y	Y	Y
0000495	Controller Information related	and	Optimum period to be around 30 hours between recharges (FMECA V6 Risk 9.4)	Y	Y	Y
0000494	Controller Information related	and	Secondary cells must not be used shall not be used (FMECA V6 Risk 9.4)	Y	Y	Y
0000493	Controller Information	and	Batteries to be properly characterised for diving, including the error in predicting battery	Y	Y	Y

	related	life (FMECA V6 Risk 9.4)			
0000492	Controller Information related and	Swept power drop out test to shall be used to check Brown Out Circuit activation (FMECA V6 Risk 9.3)	Y	Y	Y
0000491	Controller Information related and	Batteries shall be soldered, contacts are not acceptable (FMECA V6 Risk 9.3)	Y	Y	Y
0000490	Controller Information related and	Batteries state shall be shown during power-up sequence (FMECA V6 Risk 9.2)	Y	Y	Y
0000489	Controller Information related and	Dives with an adequate batteries capacity (10 hours minimum) shall not be allowed (FMECA V6 Risk 9.1, 9.2)	Y	Y	Y
0000488	Loop Volume Relief related	User shall not switch OPV with ALV accidentally (FMECA V6 Risk 8.11)	Y	Y	Y
0000487	Loop Volume Relief related	OPVs shall not be used as water traps (FMECA V6 Risk 8.10)	Y	Y	Y
0000486	Loop Volume Relief related	OPV operation to be verified (FMECA V6 Risk 8.9)	Y	Y	Y
0000485	Loop Volume Relief related	OPV shall be robust (FMECA V6 Risk 8.8)	Y	Y	Y
0000484	Loop Volume Relief related	OPV shall be positioned as close to the lung centroid as possible (FMECA V6 Risk 8.7)	Y	Y	Y
0000483	Loop Volume Relief related	OPV cracking pressure shall be checked as part of pre-dive positive pressure check (FMECA V6 Risk 8.6)	Y	Y	Y
0000482	Loop Volume Relief related	OPV to be positioned so it cannot be adjusted accidentally during dive (FMECA V6 Risk 8.6)	Y	Y	Y
0000481	Loop Volume Relief related	OPV to be located where it cannot be changed accidentally during dive (FMECA V6 Risk 8.5)	Y	Y	Y
0000480	Loop Volume Relief related	All O-ring designs shall be checked as part of mechanical design review checklist (FMECA V6 Risk 8.4)	Y	Y	Y
0000479	Loop Volume Relief related	A filter to be fitted to both inside and outside the OPV membrane/diaphragm (FMECA V6 Risk 8.3)	Y	Y	Y
0000478	Loop Volume Relief related	OPV shall be a dual membrane (FMECA V6 Risk 8.3)	Y	Y	Y
0000477	Loop Volume Relief related	OPV to be fully characterised (FMECA V6 Risk 8.2, 8.3)	Y	Y	Y

0000476	Loop Volume Relief related	Active control over pre-dive positive pressure checks shall be indicated (FMECA V6 Risk 8.1)	Y	Y	Y
0000475	Loop Volume Sufficiency related	Counterlungs shall be fixed down so they cannot trap themselves or kink (FMECA V6 Risk 7.10)	Y	Y	Y
0000474	Loop Volume Sufficiency related	Gas paths in the counterlung to be protected such that the counterlung cannot block the gas exit ports (FMECA V6 Risk 7.10)	Y	Y	Y
0000473	Loop Volume Sufficiency related	Counterlung capacity shall be between 5l and 6l (FMECA V6 Risk 7.10)	Y	Y	Y
0000472	Loop Volume Sufficiency related	ALV and BOV should not have any means to turn it off (FMECA V6 Risk 7.9)	Y	Y	Y
0000466	Loop Volume Sufficiency related	Make-Up-Gas contents shall be monitored and checked for leakage pre-dive (FMECA V6 Risk 7.5, 7.8, 7.9)	Y	Y	Y
0000471	Loop Volume Sufficiency related	Diver to be advised not to use gas with a CNS or narcosis risk at the greatest depth (FMECA V6 Risk 7.7)	Y	Y	Y
0000470	Loop Volume Sufficiency related	Gas switch blocks shall be eliminated (FMECA V6 Risk 7.7)	Y	Y	Y
0000469	Loop Volume Sufficiency related	Make-Up-Gas shall be monitored during descent and END shall be monitored (FMECA V6 Risk 7.7)	Y	Y	Y
0000468	Loop Volume Sufficiency related	Independent bail-out to be used (FMECA V6 Risk 7.6)	Y	Y	Y
0000467	Loop Volume Sufficiency related	ALV shall be used (FMECA V6 Risk 7.6)	Y	Y	Y
0000463	Loop Volume Sufficiency related	A rapid drop of Make-Up-Gas pressure to be detected by the system (FMECA V6 Risk 7.3)	Y	Y	Y
0000454	Oxygen Insufficiency related	Hypoxic Make-Up-Gas shall be run via a manifold and not used near the surface (FMECA V6 Risk 6.20)	Y	Y	Y
0000455	Oxygen Insufficiency related	Make-Up-Gas gases to be detected and decline the dive if hypoxic on surface.(FMECA V6 Risk 6.20)	Y	Y	Y

0000456	Oxygen Insufficiency related	PPO2 shall be 0.7 or above to start dive (FMECA V6 Risk 6.20)	Y	Y	Y
0000457	Oxygen Insufficiency related	ALV injection rate shall be limited to 12l/min (FMECA V6 Risk 6.20)	Y	Y	Y
0000459	Oxygen Insufficiency related	Right to left loop flow to be used (FMECA V6 Risk 6.22)	Y	Y	Y
0000461	Oxygen Insufficiency related	PPO2 level to be monitored and automatic bail out shall be provided if the PPO2 cannot be maintained (FMECA V6 Risk 6.24)	Y	Y	Y
0000460	Oxygen Insufficiency related	OPV shall be fitted only to the inhale counterlung or inhale hose between inhale counterlung and mouthpiece(FMECA V6, Risk 6.23)	Y	Y	Y
0000462	Loop Volume Sufficiency related	Make-Up-Gas pressure shall be monitored by the system (FMECA V6 Risk 7.1, 7.2, 7.3)	Y	Y	Y
0000458	Oxygen Insufficiency related	Hyperoxic Make-Up-Gass shall be run via a manifold and be switched out at depth (FMECA V6 Risk 6.21)	Y	Y	Y
0000453	Oxygen Insufficiency related	O2 injector shall provide 12l/min of O2 (FMECA V6 Risk 6.19, 6.20, 6.21)	Y	Y	Y
0000445	Oxygen Insufficiency related	Rebreather shall run as pure O2 rebreather automatically when above 6m (FMECA V6 Risk 6.15, 6.19)	Y	Y	Y
0000452	Oxygen Insufficiency related	Manual flush rate shall be limited so that user cannot reduce the PPO2 to below 0.2 (FMECA V6 Risk 6.18)	Y	Y	Y
0000447	Oxygen Insufficiency related	O2 injector shall keep breathing loop at full pressure at maximum rate of ascent (120m/min) (FMECA V6 Risk 6.16, 6.17, 6.18)	Y	Y	Y
0000451	Oxygen Insufficiency related	Suit and BCD supplies to be quick release (FMECA V6 Risk 6.17)	Y	Y	Y
0000450	Oxygen Insufficiency related	PPO2 set points which are lower than the corresponding fraction of O2 in air shall not be allowed (FMECA V6 6.17)	Y	Y	Y
0000448	Oxygen Insufficiency	Torpedo and fast ascent tests to be included in rebreather verification (FMECA V6 Risk 6.16,	Y	Y	Y

	related	6.17)			
0000432	Oxygen Insufficiency related	Auto bailout and shutoff valve to be fitted (FMECA V6 Risks 6.6, 6.7, 6.11)	Y	Y	Y
0000431	Oxygen Insufficiency related	Oxygen injector to be a variable orifice valve (FMECA V6 Risks 6.6, 6.7, 6.12)	Y	Y	Y
0000449	Oxygen Insufficiency related	OPV to be placed between the inhale CL and mouthpiece (FMECA V6 Risk 6.16, 6.17)	Y	Y	Y
0000446	Oxygen Insufficiency related	Manual gas injection shall be eliminated when Make-Up-Gas used during ascent to surface (FMECA V6 Risk 6.16)	Y	Y	Y
0000444	Oxygen Insufficiency related	Make-Up-Gas gases to be detected (FMECA V6 Risk 6.15)	Y	Y	Y
0000443	Oxygen Insufficiency related	User to be required to Flush or ascend if PPO2 increases over set point if second motor driver is connected (FMECA V6 Risk 6.13)	Y	Y	Y
0000442	Oxygen Insufficiency related	Second driver to be connected in case of O2 orifice motor driver failure (FMECA V6 risk 6.13)	Y	Y	Y
0000441	Oxygen Insufficiency related	O2 orifice motor driver failure to be detected automatically (FMECA V6 Risk 6.13)	Y	Y	Y
0000440	Oxygen Insufficiency related	Oxygen injector shall operate with both compensated and non-compensated regulators (FMECA V6 Risk 6.12)	Y	Y	Y
0000439	Oxygen Insufficiency related	Full safety verification and assessment to be carried out to ensure O2 injector operates correctly (FMECA V6 Risk 6.12)	Y	Y	Y
0000426	Oxygen Insufficiency related	Oxygen injector and oxygen cylinder pressure to be monitored by the system(FMECA V6 Risk 6.2)	Y	Y	Y
0000438	Oxygen Insufficiency related	Voice annunciationof the resulting low PPO2 level to be used (FMECA V6 Risk 6.11)	Y	Y	Y
0000437	Oxygen Insufficiency related	Oxygen composition to be checked before every dive (FMECA V6 Risk 6.11)	Y	Y	Y
0000436	Oxygen Insufficiency	Oxygen assesment to be verified (FMECA V6 Risk 6.10)	Y	Y	Y

	related				
0000435	Oxygen Insufficiency related	All materials, flows and components in contact with oxygen to have full oxygen assesment (FMECA V6 Risk 6.10)	Y	Y	Y
0000434	Oxygen Insufficiency related	Oxygen injector to be checked during positive pressure test at startup (FMECA V6 Risk 6.9)	Y	Y	Y
0000433	Oxygen Insufficiency related	Oxygen sensors to be calibrated in air (FMECA V6 6.9)	Y	Y	Y
0000430	Oxygen Insufficiency related	Umbilical UBA shall have umbilical gas, or gas supply sensor (FMECA V6 Risk 6.5)	Y	Y	Y
0000429	Oxygen Insufficiency related	Oxygen usage to be monitored (FMECA V6 Risk 6.5)	Y	Y	Y
0000427	Oxygen Insufficiency related	Hard plastic knobs with a surface that is less likely to move with friction shall be used on oxygen cylinders(FMECA V6 Risk 6.2)	Y	Y	Y
0000425	Oxygen Insufficiency related	Oxygen cylinder cannot be switched off prior to the unit being switched on (FMECA V6 Risk 6.2)	Y	Y	Y
0000424	Oxygen Insufficiency related	Diver shall be warned when hypoxic Make-Up-Gas is used(FMECA V6 Risk 6.1)	Y	Y	Y
0000423	Oxygen Insufficiency related	Diving with oxygen cylinders empty shall be managed and avoided(FMECA V6 Risk 6.1)	Y	Y	Y
0000419	Cylinder related	Cylinder regulator O-ring shall be oxygen compatible material (FMECA V6 Risk 5.7)	Y	Y	Y
0000418	Cylinder related	Cylinder valve O-ring shall be oxygen compatible material (FMECA V6 Risk 5.7)	Y	Y	Y
0000417	Cylinder related	The loss of gas from cylinder during dive recovery action shall be in the user manual(FMECA V6 Risk 5.6)	Y	Y	Y
0000416	Cylinder related	Cylinder valves compliance to ISO 10297-2006(e) (FMECA V6 Risk 5.6)	Y	Y	Y
0000415	Cylinder related	Cylinders shall be protected from detritus (FMECA V6 Risk 5.5).	Y	Y	Y
0000414	Cylinder related	Helium shall not be stored in the carbon wrapped cylinders for a long periods (FMECA V6 Risk 5.4)	Y	Y	Y

0000413	Cylinder related	Carbon wrapped cylinders annual inspection requirement to be in the user manual (FMECA V6 Risk 5.4)	Y	Y	Y
0000412	Cylinder related	Plastic cored cylinders shall not be used (FMECA V6 Risk 5.3)	Y	Y	Y
0000410	Cylinder related	Carbon wrapped cylinder coating (FMECA V6 Risk 5.2)	Y	Y	Y
0000370	Other sensing	gas Oxygen Cylinder Contents (Pressure) measurement	Y	Y	Y
0000397	Environment conditions	Helium tolerance	Y	Y	Y
0000368	Other sensing	gas Helium measurement	Y	Y	Y
0000390	Environment conditions	EMC Requirements	Y	Y	Y
0000369	Operating duration related	Temperature sensors are required on the Scrubber Stick to predict scrubber life.	Y	Y	Y
0000374	Environment conditions	Temperature sensors are required on the Sensors Card for ambient temperature measurements	Y	Y	Y
0000376	Interface related	Communications requirements	Y	Y	Y
0000378	Environment conditions	Carbon Monoxide sensor is required for the umbilical rebreather	Y	Y	Y
0000380	Operating duration related	Factory service interval shall be one year and enforced	Y	Y	Y
0000394	Environment conditions	All connectors outside the rebreather, shall be wet mateable	Y	Y	Y
0000393	Environment conditions	Power supplies: batteries shall be disconnectable	Y	Y	Y
0000392	Environment conditions	Power supplies: batteries shall either not be pressurised, or shall be under 5mm thick and characterised for extreme pressure	Y	Y	Y
0000391	Environment conditions	Power supplies: cells thicker than 5mm shall be Lithium Phosphate type	Y	Y	Y
0000381	Environment conditions	Power supply duration	Y	Y	Y
0000367	Flood prevention	Electronic modules on rebreathers shall detect when the rebreather is open	Y	Y	Y
0000388	PPO2 Related	When PPO2 level is controlled, it shall have a	Y	Y	Y

		maximum error of +/- 0.09 bar at constant depth			
0000389	PPO2 Related	PPO2 level shall be limited to $0.2 < PPO2 < 2.0$ always	Y	Y	Y
0000382	Flood prevention	Flood detection is required on all rebreathers with electronics (i.e. within ALARP)	Y	Y	Y
0000383	Interface related	Every independent electronic unit shall log every second of every dive for all dives between factory service intervals	Y	Y	Y
0000387	PPO2 Related	PPO2 level shall be reported to the PPO2 controller with a resolution of 0.001 ATM	Y	Y	Y
0000385	PPO2 Related	PPO2 level shall be reported to the diver/supervisor with an resolution of 0.05 ATM with recourse to a display with 0.01 ATM	Y	Y	Y
0000386	PPO2 Related	PPO2 level reporting frequency to the diver/supervisor shall be every second, with over-ride for on demand displays	Y	Y	Y
0000379	Operating duration related	Base Unit electronics shall have MTBCF of 1 billion hours	Y	Y	Y
0000358	PPO2 Related	ALVBOV needs to be actuated electronically by the PFD	Y	Y	Y
0000351	Ergonomic related	ALVBOV Requirements, Top level	Y	Y	Y
0000350	PPCO2 Related	ALVBOV in O.C. mode must comply with EN250 at 50msw	Y	Y	Y
0000348	Flood prevention	ALVBOV must completely close the rebreather breathing loop when ALVBOV is in O.C. mode	Y	Y	Y
0000347	Flood prevention	ALVBOV must have auto-close to shut rebreather loop when out of the mouth	Y	Y	Y
0000384	PPO2 Related	PPO2 level shall be reported to the diver or supervisor with an accuracy of 0.0243 ATM	Y	Y	Y
0000365	PPO2 Related	PPO2 level shall be reported to the diver or supervisor over the range 0 to 2.5 ATM	Y	Y	Y
0000375	Environment conditions	Ambient pressure sensors on the Sensors Card and in the Base Unit	Y	Y	Y
0000372	Other sensing	gas Make-Up-Gas pressure measuring	Y	Y	Y
0000371	Environment conditions	Humidity sensor is required	Y	Y	Y
0000366	PPCO2 Related	CO2 Measuring: Initial requirements	Y	Y	Y

0000364	Environment conditions	All electronics with batteries must be chargeable via a USB 2.0 connector with both low and high current sources	Y	Y	Y
0000359	Environment conditions	Storage temperature range -30C to +70C	Y	Y	Y
0000363	Environment conditions	Subset Operating Temperature range in of electronics is -30C to +70C, to error that rebreather is outside operating range	Y	Y	Y
0000361	Environment conditions	Operating Temperature range in air of electronics is 2C to 70C, under which conditions electronics shall be in full calibration	Y	Y	Y
0000362	Environment conditions	Operating temperature range underwater of Surface Supplied rebreather with gas heating, is -4C to +34C	Y	Y	Y
0000360	Environment conditions	Operating temperature range underwater without gas heating, is +4C to +34C	Y	Y	Y
0000311	PPO2 Related	O2 cell fault tolerance	Y	Y	Y

6 EN 61508 AUDIT

An extensive audit was carried out on Deep Life’s lifecycle processes using the Open Revolution family of products as the case study, by a team of auditors from SIRA Certification from December 2008 to April 2009.

The opinion of the auditors familiar with the dive industry and the application, is the equipment is safe, certifiable and is likely to provide a substantial increase in safety.

Deep Life is completing an EN 61508 process compliance qualification and will certify this equipment, when certified to do so by SIRA, as implementing best practice, and meeting ALARP based on the evidence here, in the other volumes of the FMECA and on the whole of the safety case for the three models of the Open Revolution family of rebreather products.

7 CONCLUSION

The Open Revolution family of rebreather products implement best practice and implements ALARP principles.

Diving is an inherently hazardous and high risk activity. The equipment itself reduces those risks compared to contemporary state of the art equipment and methods, and provides broad spectrum protection to the diver.

Deep Life is seeking certification of the product to EC PPE Directives and EN 14143:2003 from SGS UK Ltd as a PPE Notified Body.