

REBREATHER FAILURE MODES AND THEIR IMPLICATIONS FOR COMPLAINT WITH EN61508

DOCUMENT NUMBER: FMECA_OR_Faults_060807.doc
 ORIGINATOR: Dr. Alex Deas, Dr. Bob Davidov, Marat Evtukov, Alexei Bogatchov, Dr. Sergei Malyutin, Dr Vladimir Komarov, Dr Oleg Zabgreblenny, Dr Alexander Kudriashov
 DEPARTMENT: Engineering
 REV ORIGINATED: 1st August 2006
 REVISION: B1

APPROVALS	
____ AB _____ Hardware Architect	____ 2 Aug 2006 _____ Date
____ N/A _____ Software Architect	____ _____ Date
____ ME _____ Project Manager	____ 1 Aug 2006 _____ Date
____ VK _____ Quality Officer	____ 2 Aug 2006 _____ Date

Controlled
Document

Classified Document
DO NOT COPY.

Revision History

Revision	Date	Description
A	1 st Aug 2004	Case initialised.
B	2 nd August 2006	Review. Inclusion of section for Commercial Dive Config. B1 with item 7.13.

Copyright 2004, 2006 © Deep Life Ltd.

All information and data provided herein are for general information purposes only and are subject to change without notice or obligation.

Table of Contents

1 Purpose and Scope.....	5
2 Verification.....	5
3 Structure.....	6
4 Adoption of Results.....	6
5 Oxygen Supply Failures.....	6
5.1 Oxygen Cylinder Empty.....	6
5.2 Oxygen Cylinder Switched Off.....	7
5.3 Oxygen First Stage Failure.....	7
5.4 Oxygen First Stage Over Pressure.....	8
5.5 Oxygen Hose Leaks.....	8
5.6 Oxygen Solenoid Stuck Open.....	9
5.7 Oxygen Solenoid Stuck Closed.....	9
5.8 Oxygen Manual Injector Failure.....	10
5.9 Wrong Gas in Oxygen cylinder.....	10
5.10 Oxygen fire.....	11
5.11 Calibration using wrong gas.....	11
5.12 Solenoid Stuck Shut, due to rise in Intermediate Pressure.....	12
5.13 O2 orifice motor driver failure.....	12
5.14 Use of O2 instead of DIL, using hypoxic DIL, to excess depth.....	13
5.15 Use of hypoxic DIL in ascent to surface.....	13
5.16 Uncontrolled ascent (max 120m/min) with low PPO2.....	13
5.17 PPO2 low due to injection not keeping up with demand.....	14
5.18 Low PPO2 set point followed by rapid ascent.....	14
6 Diluent Supply Failures.....	15
6.1 Diluent Cylinder Empty.....	15
6.2 Diluent Cylinder Switched Off.....	15
6.3 Diluent First Stage Failure.....	16
6.4 Diluent First Stage Over Pressure.....	16
6.5 Diluent Hose Leaks.....	17
6.6 Diluent Manual Injector Failure.....	17
6.7 Wrong Gas In Diluent Cylinder.....	18
6.8 Alternate Air Source Free Flow.....	18
7 Controller Failures.....	19
7.1 Battery Low.....	19
7.2 Battery Failure.....	19
7.3 Battery Bounce.....	20
7.4 Handset failure apparent to user.....	20

7.5 Handset or Controller Hangs.....	21
7.6 Handsets Switched off.....	22
7.7 Oil Filled Chamber Leaks Oil.....	23
7.8 Electronic Component Explodes.....	23
7.9 User unaware of failure message or unable to act.....	24
7.10 Faulty Software.....	25
7.11 Handsets Misread.....	25
7.12 Cracked Electronics Housing.....	26
7.13 Corroded wiring.....	26
8 Oxygen Sensor Failures.....	27
8.1 O2 Cell Decompression Failure.....	27
8.2 O2 Cell has CO2 Contamination.....	28
8.3 O2 Cell Contamination.....	28
8.4 O2 Cell Thermal compensation failure.....	29
8.5 O2 Cell Loose Connection.....	29
8.6 O2 Single Cell Failure.....	30
8.7 O2 Two Cell Failure.....	30
8.8 O2 Cell Failures Tracked Incorrectly.....	31
8.9 O2 Cell Calibration Incorrect.....	31
8.10 O2 Cells show different reading to independent PPO2 monitor.....	31
8.11 O2 Cells have condensation on sensor face.....	32
8.12 O2 Cells have differential pressure applied.....	32
8.13 O2 Cell Explodes.....	33
9 Diver Failures.....	33
9.1 Breathing off loop that cannot sustain life.....	33
10 CO2 Related Failures.....	34
10.1 Scrubber Not Fitted.....	34
10.2 Scrubber Physically Damaged, affecting gas X-section.....	34
10.3 Scrubber Exhausted.....	35
10.4 Scrubber Bypass.....	36
10.5 Excess Work of Breathing.....	36
10.6 Counterlungs change position, causing CO2 hit.....	37
10.7 One Way Valve Stuck Open.....	37
10.8 One Way Valve Stuck Shut.....	38
11 Other Failures.....	39
11.1 Allergic Reaction to Material.....	39
11.2 BC Failure.....	39
11.3 Harness Failure.....	40
11.4 Loop Flood.....	40
11.5 Pressure Sensor Failure.....	41

11.6 Gross dry suit leak.....	41
11.7 Counter-diffusion hazard.....	42
11.8 Noxious chemical off-gassing.....	42
11.9 Vomiting into breathing loop.....	42
11.10 Deco dive with incorrect PPO2 level in loop.....	43
11.11 DCS risk higher than statistical projection of deco algorithm.....	43
11.12 CNS Toxicity.....	43
12 Failures Specific To Surface-Supplied Dives.....	44
12.1 Loss of Umbilical (Commercial diver).....	44
12.2 Cut of umbilical near surface (Commercial Diver).....	45
12.3 Entrapment of Umbilical (Commercial diver).....	45
12.4 Loss of Helmet (Commercial diver).....	45
12.5 Sudden change in depth (Commercial diver).....	46
12.6 CO in loop (Commercial diver).....	46
12.7 HC or Volatile Organic Compounds in Loop (Commercial diver).....	46
12.8 Loss of communications (Commercial Diver).....	46
12.9 Loss of Suit Heating (Commercial diver).....	47
12.10 Excess suit heating (Commercial diver).....	47
13 General Diving Hazards.....	47
References:.....	51

1 PURPOSE AND SCOPE

This document provides the framework for the detailed Failure Mode Effect and Criticality Analysis for the Open Revolution rebreather submissions developed by Deep Life Ltd.

This list is compiled from accident analyses, failure analyses of contemporary equipment and formal verification modelling of rebreathers and their environment.

The document is intended to be an exhaustive list of the safety-related failure modes of rebreathers, for two purposes:

- 1.To provide a list of failures, against which each component in a rebreather can be examined and referenced in HAZOP studies, carried out during a rebreather design. The result of those HAZOP studies, carried out at a component-by-component level and referring to the faults in this document, with suitable MTBF/MTBCF calculations, will form an FMECA of the system to the standard required by EN14143:2003 and EN61508.

- 2.To provide a structured framework for the analysis of equipment after an accident to determine whether or not the equipment contributed to, or caused, the accident.

All references to “the equipment” carrying out a positive action refer to the equipment detailed in the Open Rebreather submission by Deep Life Ltd. Other equipment may perform an alternative action, or no action: this is up to the verification team associated with that equipment to determine.

All references to “the system” refer to the Open Revolution submission by Deep Life Ltd. References to “mandatory checks” refer to the pre-dive checks performed by that specific rebreather controller.

This is a working engineering document, rather than an academic tome: it should be revised as new information becomes available.

2 VERIFICATION

The failure modes listed in this document are drawn from numerous sources, the prime sources being listed in [1] to [7] in the references. Other sources include FMECA studies on contemporary equipment, rebreather internet forums, coroner reports, equipment failure reports issued by public health laboratories, warnings issued by rebreather manufacturers. Accident appraisal advice from other rebreather manufacturers are a further important source of failure information used in compiling this document.

Each fault mode attributable to equipment has been encoded in a formal fault model in the Open Revolution rebreather environment. This model is a Matlab model, which has been published by Deep Life Ltd to enable the safety of new rebreather designs to be verified.

The formal verification environment allows any of these faults to be selected, combined with any other(s), and then applied to verify the safety performance of the equipment under these fault conditions.

Efforts have been made to encourage other manufacturers to use, critique and extend these formal models. There has been some independent review of the models by others working on rebreather design. The objective is to create an industry-wide consensus on the formal fault models needed to verify the safe operation of rebreather apparatus.

3 STRUCTURE

This report classifies faults into groups, based on the section of the equipment associated with the failure.

There is an inevitable duplication of some failures. For example, breathing bags (counterlungs) becoming detached is one failure, but it is also listed under WOB increase in the section on PPCO2 Control, as breathing bag detachment is one cause of such an increase. The view was taken that it is better to include duplication than miss critical failure modes. This approach also simplifies the use of the fault list in HAZOP reviews.

4 ADOPTION OF RESULTS

The Open Revolution submission from Deep Life incorporates all of the recommendations made in this document under the EN61508 Implications. The submission itself has been developed through a design process meeting EN61508.

5 OXYGEN SUPPLY FAILURES

5.1 Oxygen Cylinder Empty

Cause & Prevention

Use of empty cylinder: will not pass pre-dive checks but user could dive anyway.

Diving with not enough O2 for the dive: system enforces dive abort when O2 consumption and O2 remaining do not allow user to reach surface with 50 bar in tank.

A leak. System enforces abort when insufficient O2.

Hose failure from O2. Forces bail-out and abort of dive.

First Stage Failure, including over-pressure relief, O2 ring failure. Forces bail-out, and abort of dive. Dive abort can be on Semi-Closed. This situation is the worst-case test case for Auto-ShutOff valve control.

Symptoms

Surface

Will not pass mandatory pre-dive checks.

Dive

Failure to hold set point. Low O2 Alarm sounding. Oxygen contents gauge showing low.

Recovery action during Dive

Diver must avoid this situation. Bail-out onto DIL, but check DIL is normoxic.

EN61508 Implication

System manages each failure mode, and where not recoverable, forces Bail-out to open circuit or diluent flush-and-fly unit in semi-closed mode.

Important that user is not allowed to dive unless there is enough O₂ to reach the surface, including deco. System should monitor DIL and O₂ levels. O₂ fraction should not be allowed to drop below that of air at the same depth, and projection should use a 1.76l/min of O₂ in calculating this availability, plus the loss of gas during ascent (using the known maximum dead volume of the loop).

Issue where hypoxic DIL is used is a serious one: diver must be warned.

5.2 Oxygen Cylinder Switched Off

Cause

Switched off on dive boat after pre-dive checks, and forgetting to switch on again.

O₂ cylinder accidentally turned off during dive, due to handle rubbing on something. Condition is detected by software, showing a cylinder content falling more rapidly than O₂ is being used. This is the worst-case test case for the Injector-led O₂ injection control system.

Symptoms

Handled, in case of Low O₂, by the Injector-led O₂ controller finding an imbalance between injected gas and measured gas, then going into diagnostic mode, finding that injecting gas causes no gas, and treats failure first as a cylinder-valve-shut failure, then, if user confirms valve is open, as an injector failure. If second injector has same fault, requests user to turn on cylinder valve.

Recovery action during Dive

Urgent. Open O₂ valve, ready to bail out to open circuit or diluent flush-and-fly unit in semi-closed mode. User is advised of this action, and system forces it with the Auto ShutOff valve.

Preventative action

This is a common fault, as the O₂ valve knob sticks out from the cylinder and is easily rubbed. The worst position is when the O₂ cylinder is hung like a stage, when the valve rubs on clothing.

Check position of valve and ensure it is covered, but still accessible.

EN61508 Implication

System should not allow the oxygen cylinder to be switched off prior to the unit being switched on, unless the unit is already underwater when it is switched on, in which case the situation is handled as during the dive, as described below.

System must monitor O₂ injector and O₂ pressure. Where a mismatch occurs, the error message should be specifically "O₂ Tank Valve is Closed. Open it!" Requires a digital contents gauge on the O₂ and DIL tanks coupled to the CCR controller.

5.3 Oxygen First Stage Failure

Same as cylinder contents empty, but sudden onset.

This fault mode includes other causes, such as the 15 micron filter being blocked prior to the O2 injectors, blockage of all O2 injectors. All have the same effect.

5.4 Oxygen First Stage Over Pressure

Cause

Poor maintenance, wear of first stage, corrosion or contamination.

Symptoms

Surface

Only if battery low. Solenoid can fail to fire before low battery warning given. Hence failure to calibrate. Failure to hold set point during pre-breathe. Low O2 Alarm Sounding.

Dive

Only if battery low. Solenoid can fail to fire before low battery warning given. Hence failure to hold set point during pre-breathe. Low O2 Alarm Sounding.

Recovery action during Dive

Urgent. Bail out to open circuit or diluent flush-and-fly unit in semi-closed mode.

Preventative action

Check interstage pressure during servicing and use fresh batteries.

EN61508 Implication

Verify the O2 injector works for all possible O2 intermediate pressures.

5.5 Oxygen Hose Leaks

Cause

Wear, poor maintenance.

Symptoms

Surface

Failure to calibrate. Failure to hold set point during pre-breathe. Low O2 Alarm Sounding. Oxygen contents gauge showing low or audible air loss from cylinder.

Dive

Failure to hold set point. Low O2 Alarm sounding. Oxygen contents gauge may show empty. Bubbles in water.

Recovery action during Dive

Urgent. Bail out to open circuit or diluent flush-and-fly unit in semi-closed mode.

Preventative action

Pre-dive checks.

EN61508 Implication

Monitor O2 usage (requires O2 contents gauge and declaration of tank size). Give specific warning of leaking hose.

5.6 Oxygen Solenoid Stuck Open

Cause

Corrosion, poor maintenance, salt crystals or contaminates in unit. High Interstage pressure. Low Battery.

Symptoms

Surface

Failure to calibrate. Failure to hold set point during pre-breathe. High O2 Alarm Sounding. Counter lungs full.

Dive

Failure to hold set point. High O2 Alarm sounding. Excessive buoyancy. Can hear solenoid injecting at all times.

Recovery action during Dive

Urgent. Close O2 valve. Bail out, or diluent flush.
Option to fly manually using O2 valve or to go semi-closed.

Preventative action

Regular service. Lube and ensure solenoid clean. Check mesh filter above solenoid. Recharge Batteries.

EN61508 Implication

The oxygen injector should not be a solenoid, but a variable orifice valve, so that when it fails, the failure state maintains the average oxygen consumption.

Fit an Auto bailout and shutoff valve.

5.7 Oxygen Solenoid Stuck Closed

Cause

Corrosion, poor maintenance, salt crystals or contaminates in unit. Low battery. High interstage pressure

Symptoms

Surface

Failure to calibrate. Failure to hold set point during pre-breathe. Low O2 Alarm Sounding.

Dive

Failure to hold set point. Low O2 Alarm sounding.

Recovery action during Dive

Urgent. Fly unit manually using manual O2 injector. Consider bail-out.

Preventative action

Regular service. Lube and ensure solenoid clean. Check mesh filter above solenoid. Fresh batteries.

EN61508 Implication

The oxygen injector should not be a solenoid, but a variable orifice valve, so that when it fails, the failure state maintains the average oxygen consumption.

Fit an Auto bailout and shutoff valve.

5.8 Oxygen Manual Injector Failure

Cause

Poor maintenance. Failure to plug hose on properly.

Symptoms

Surface

Failure of pre dive checks.

Dive

Loss of gas from loop, flooding of loop.

Recovery action during Dive

Urgent. Reconnect Hose or re-screw injector down. Bail out if loop flooded.

Preventative action

Pre-Dive checks.

EN61508 Implication

Eliminate the failure point: Design out the manual O2 injector.

5.9 Wrong Gas in Oxygen cylinder

Cause

Nitrox fill or gas other than 100% oxygen.

Symptoms

Surface

Failure to calibrate (maybe). Failure to hold set point. Lungs full.

Dive

Failure to hold set point (maybe). Excessive buoyancy and injector function.

Recovery action during Dive

Bail out (diver does not know what gas he is breathing).

Preventative action

ALWAYS analyse your gases after a fill.

EN61508 Implication

Calibrate the O2 Cells in air (by detecting when the scrubber can is open). Make provision for saturation environments.

Check the O2 injector by a positive pressure test during startup, and check O2 Cell response is as expected.

5.10 Oxygen fire

Cause

Poor O2 handling.
Contamination.
Poor maintenance.
Unsuitable materials.

Preventative action

Proper design and maintenance procedures.
Proper training of operators.
Use gases with 23% less O2.

EN61508 Implication

Ensure all materials in breathing loop and all materials in contact with high-pressure oxygen are O2 compatible, as listed by the latest available NASA O2 compatibility report.

5.11 Calibration using wrong gas

Cause

User error and design omission allowed user to dive with 60% O2 in cylinder used as 100% O2. Almost a fatality in both cases.

Preventative action

Calibrate using air when scrubber is open, then check during descent near surface.

EN61508 Implication

Rebreather itself should check the O2 composition before every dive. It has calibrated O2 Cells (if the recommendation to force calibration in air is followed), and can inject O2 and check the composition of the loop gas on the surface to give an injector call. It is not complex to compensate the injector call for depth, so that no gas switch can introduce a low FO2 gas.

Auto Shut Off Valve would have prevented the problem affecting the diver's safety.

Voice annunciation of the resulting low PPO2 level would have prevented the problem affecting the diver's safety.

5.12 Solenoid Stuck Shut, due to rise in Intermediate Pressure

Cause

Rapid ascent in combination with O2 solenoid having narrow operating range.

Preventative action

Eliminate O2 solenoids.

EN61508 Implication

Carry out a full safety verification and assessment of the O2 injector to ensure it operates correctly with all possible intermediate pressures.

5.13 O2 orifice motor driver failure

Cause

Poor maintenance, or failure of component: motor, position sensor, etc.

Symptoms

Surface

PPO2 should not equal 0.7ATA.

Should be detected automatically, as PPO2 level changes but the output of the position sensor is constant.

Dive

Should be detected automatically, as PPO2 level changes but the output of the position sensor is constant.

Recovery action during Dive

None required if system recovery is sufficient. If second unit fails, then bail out.

Preventative action

Check motor operational range during self check sequence.

EN61508 Implication

Should be detected automatically, as PPO2 level changes but the output of the position sensor is constant.

System should connect the second driver to the control loop and user is advised of this action.

Urgent (when PPO2 level increases beyond the set point after the connection of the second driver), user should be required to Flush or ascend.

5.14 Use of O2 instead of DIL, using hypoxic DIL, to excess depth

Cause

Untrained diver using hypoxic diluent, and pure O2 above hyperoxic depth.

Preventative action

Proper training and experience in buoyancy control.

EN61508 Implication

Eliminate manual O2 injection.

Detect what the DIL gases are and run as a pure O2 rebreather automatically when above 6m.

5.15 Use of hypoxic DIL in ascent to surface

Cause

Loss of O2.

Use of wrong bail-out gas.

Use of wrong cylinder of gas.

Poor training.

Preventative action

Monitor O2 and DIL gases.

EN61508 Implication

Eliminate manual gas injection.

Ensure O2 injector can keep breathing loop at full pressure at maximum rate of ascent (120m/min). Include torpedo test and fast ascent test in O2 injector verification.

5.16 Uncontrolled ascent (max 120m/min) with low PPO2

Cause

Loss of weight belt.

Catastrophic failure of buoyancy control device or injector.

Entanglement with a towed object.

Entanglement with an SMB or lift bag.

Preventative action

Improved training to handle SMBs and Lift Bags properly.

Keep weight belts to simple belts rather than weight jackets.

EN61508 Implication

Covered by “end to end” clause.

Ensure PPO2 can be maintained with 120m/min ascent rates by specific inclusion in O2 injector verification plan.

To avoid this fault, the rebreather should not allow PPO2 set points which are lower than the corresponding fraction of O2 in air, until it

becomes necessary to limit CNS exposure. Use of PPO2 not less than air, to at least 30m, is recommended.

5.17 PPO2 low due to injection not keeping up with demand

Cause

User error and design limitation.
User flushes loop with hypoxic diluent.
Overlap with some other errors, such as running out of O2 or injector failure.

Symptoms

Dive

Gasping.

Recovery action during Dive

Control software should check the rate of the depth sensor and PPO2 cells and reject slow sensors.

Preventative action

User is advised to decrease the ascending rate. Service regularly and test /inspect.

EN61508 Implication

Eliminate design limitation: injector must be able to provide at least 12l/min of O2.

Manual flush rate must be limited so that with no O2 in diluent gas, user cannot reduce the PPO2 to below 0.2.

5.18 Low PPO2 set point followed by rapid ascent.

Cause

User error and design limitation. Implicated in several fatalities where user has a PPO2 set point of 0.4, then ascends rapidly. This is a special hazard near the surface where the diver does not have time to respond to a failure.

Recovery action during Dive

Control software should check the rate of the depth sensor and PPO2 cells and reject slow sensors.

Preventative action

The min PPO2 set point, when shallow, must allow the diver to “pop” to the surface without the PPO2 falling below 0.21.

EN61508 Implication

The rebreather should increase PPO2 to operate as a pure O2 rebreather above 6m.

The injector must be able to inject 12l/min.

6 DILUENT SUPPLY FAILURES

6.1 Diluent Cylinder Empty

Cause

Someone forgot to fill it, or a bad leak.

Symptoms

Surface

Failure of pre-dive checks, diluent contents gauge reads zero.

Dive

Lung squeeze on descent, unable to inject diluent. Auto Air Out not functional. Dry suit inflate not functional.

Recovery action during Dive

Plug in a reserve gas supply. Inflate lungs with manual O2 inject if above 6m.

Preventative action

Pre-dive checks.

EN61508 Implication

System must monitor DIL pressure. Where a mismatch, the error message should be specifically “DIL Tank Valve is Closed. Open it!”
Requires a contents gauge on the DIL tank.

6.2 Diluent Cylinder Switched Off

Cause

Valve rubbed, or forgetfulness.

Symptoms

Surface

Failure of pre-dive checks, diluent contents gauge reads zero.

Dive

Lung squeeze on descent, unable to inject diluent. Auto Air Out not functional. Dry suit inflate not functional.

Recovery action during Dive

Open valve.

Preventative action

Pre-dive checks.

EN61508 Implication

System must monitor DIL pressure. Where a mismatch, the error message should be specifically “DIL Tank Valve is Closed. Open it!”

Requires a contents gauge on the DIL tank. Force user to inject DIL in pre-dive check.

6.3 Diluent First Stage Failure

Cause

Wear or structural failure.

Symptoms

Surface

Failure of pre-dive checks, diluent contents gauge reads zero.

Dive

Lung squeeze on descent, unable to inject diluent. Auto Air Out not functional. Dry suit inflate not functional.

Recovery action during Dive

Plug in a reserve gas supply. Inflate lungs with manual O2 inject if above 6m.

Preventative action

Service correctly and pre-dive checks.

EN61508 Implication

System must monitor DIL pressure. Where a mismatch, the error message should be specifically "DIL Tank Valve is Closed. Open it!" Requires a contents gauge on the DIL tank. Valve unlikely to fail totally and suddenly. System must detect a rapid drop of pressure.

6.4 Diluent First Stage Over Pressure

Cause

Wear or structural failure. Poor adjustment.

Symptoms

Surface

Auto air free flow, BC inflation.

Dive

Auto air free flow, excessive buoyancy in BC, or dry suit, or ADV.

Recovery action during Dive

Shut down diluent valve. Manually operate when needed (shouldn't need to surface). Consider bailout if alternate supply.

Preventative action

Service correctly and pre-dive checks.

EN61508 Implication

Outside the eCCR, but the “end to end” clause in EN61508 may encompass this failure. Monitor DIL contents and check for leakage pre-dive.

6.5 Diluent Hose Leaks**Cause**

Wear. Poor maintenance.

Symptoms**Surface**

Failure of pre-dive checks. Audible gas escape. Diluent contents decreasing.

Dive

Audible gas escape. Diluent contents decreasing.

Recovery action during Dive

Abort dive.

Preventative action

Pre-dive checks and servicing.

EN61508 Implication

Outside the eCCR, but the “end to end” clause in EN61508 may encompass this failure. Monitor DIL contents and check for leakage pre-dive.

6.6 Diluent Manual Injector Failure**Cause**

Poor maintenance.
Failure to plug hose on properly.

Symptoms**Surface**

Failure of pre dive checks.

Dive

Loss of gas from loop, flooding of loop.

Recovery action during Dive

Urgent. Reconnect hose or re-screw injector down. Bail out if loop flooded.

Preventative action

Pre-Dive checks.

EN61508 Implication

Design out by using an ADV. If ADV fails, diver must bail out as there is insufficient volume of breathing gas on descent, detectable as a negative pressure in the loop compared to ambient. Instruct user to bail out.

Requires independent bail-out.

6.7 Wrong Gas In Diluent Cylinder**Cause**

Cylinder filled wrongly.

Symptoms**Surface**

None with normal pre-dive checks.

Dive

Problems maintaining set point during descent.

Recovery action during Dive

Abandon dive, or connect alternate diluent source (not likely to notice during dive).

Preventative action

Analyse ALL gases prior to use. Once unit is calibrated you can check the diluent O2 content by doing a diluent flush. This should be added as part of the pre-dive tests.

EN61508 Implication

Monitor gas during descent, and monitor END.

6.8 Alternate Air Source Free Flow**Cause**

Dirt or high diluent interstage pressure.

Symptoms**Surface**

Failure of pre-dive checks. Audible gas loss.

Dive

Audible gas loss and bubbles.

Recovery action during Dive

Disconnect Auto Air, or try shaking to reseal things. Consider aborting dive.

Preventative action

Service equipment and pre-dive checks.

EN61508 Implication

Outwith the eCCR, but covered by “end to end” clause.
Monitor DIL contents.

7 CONTROLLER FAILURES

7.1 Battery Low

Cause

Over-use, or internal failure.

Symptoms**Surface**

Low Bat warning on handset. Solenoid not functioning. Cannot maintain set point.

Dive

Low Bat warning on handset. O2 Injector not functioning. Cannot maintain set point.

Recovery action during Dive

Abort dive. Variable orifice valve should maintain PPO2 if ascent rate is slow, otherwise activate Auto Bail-out and Shut Off valve.

Preventative action

Pre-Dive checks and measure battery voltage before dives. Recharge when warning is shown or before big dive.

Fault incidence reduced by design: O.R. submission includes 3 independent power sources, two of which are maintained at 1 ATM.

EN61508 Implication

Lack of power is the Achilles Heal of electronics. Provide 3 power sources, with different drain rates, and do not allow dive unless adequate capacity (10 hours minimum).

7.2 Battery Failure

Cause

Over-use or internal failure. Water in battery compartment.

Symptoms**Surface**

No handset.

Dive

No handset. Solenoid not functioning. Cannot maintain set point.

Recovery action during Dive

Slave should take over. Abandon dive. If both fail then bail out if you have no alternative means of monitoring PPO2.

Preventative action

Pre-Dive checks and measure battery voltage before dives.

EN61508 Implication

Lack of power is the Achilles Heal of electronics.

Show battery state during power-up sequence.

Provide 3 power sources, with different drain rates, and do not allow dive unless adequate capacity (10 hours minimum).

7.3 Battery Bounce

Cause

Poor battery and contact design. Manifest when entering water by rolling backwards on to turtle shell. Momentarily disconnects batteries.

Symptoms

Surface

None.

Dive

Hanging. "Dive Now?" message and "Waiting for Data" messages.

Recovery action during Dive

Urgent. Perform start-up cycle. DO NOT CALIBRATE.

Preventative action

Design out the problem.

Always check handsets immediately after entering water.

EN61508 Implication

Battery contacts cannot meet EN61508. Design out the problem by using multiple redundant rechargeable Lithium Ion Gel batteries, soldered in.

7.4 Handset failure apparent to user

Cause

Flooding, wiring or mechanical breakage.

Symptoms

Surface

Blank screen.

Dive

Blank screen.

Recovery action during Dive

Main controller should take over. Abandon dive.

Preventative action

Protect handsets and check wiring during service.

EN61508 Implication

Perform full JTAG testing during power-up sequence.

Use multiple devices in handset, so failure of one clock or one integrated circuit should not cause loss of handset.

Provide a HUD in addition to handset.

Base unit should be automative.

7.5 Handset or Controller Hangs

Cause

Incompetent design: single processor, single clock source, single power source, no heartbeat monitor (watchdog circuits), no brownout circuit.

Symptoms

Surface

Screen should not change.

Dive

Screen should not change, no alarms.

Recovery action during Dive

Bail out.

Preventative action

Problem should be eliminated by design.

EN61508 Implication

This is a problem that occurs with some handsets examined during FMECA studies of contemporary equipment. The normal design procedures applied for safety critical systems should prevent this. The system should check automatically during normal start-up that these safety design provisions are operating correctly.

Ensure Watchdog circuit is operating by halting the clock for the Watchdog period.

Ensure Brown-Out circuit is operating by power cycle test.

Ensure state machines have redundant states to detect failure and return unit to safe operation.

Fill all unused memory locations with recovery code.

Routines should apply predicates in input data so that random jumps to the routine can be detected and recovered.

The start-up sequence should detect if an abnormal shutdown occurs, so immediate recovery can be carried out.

Any such failure should be logged and the unit permanently locked out on the surface.

The circuit should have multiple clocks, power supplies and other circuits so that the MTBCF of the circuit exceeds the SIL 4 requirement by sufficient margin to ensure that, when coupled with the MTBCF of the mechanical components, the overall MTBCF is still above 1 billion hours.

7.6 Handsets Switched off

Cause

Design fails to keep handsets switched on when unit is being used.

User often switches handset off if it fails in an obvious or dangerous manner underwater. For example, if keeps injecting O₂ despite PPO₂ being sufficient, or enters calibration mode.

Be very careful to analyse all failures where user surfaces with handsets switched off, especially with experienced users.

Symptoms

Surface

Pre-dive check failure. Blank handsets. No pre-breathe.

Dive

No handset display.

Recovery action during Dive

Bail out or die.

Preventative action

Pre-dive checks and basic monitoring of unit.

EN61508 Implication

Occurs in units where there is a failure of the electronics and user switches the handset off to try and bring the unit back up. Several cases where user has died before unit has come back up.

Solution adopted is to design out the problem: ensure unit powers on automatically whenever the PPO₂ is less than 0.19.

Eliminate all possibility that the unit can “hang”.

Provide an HUD which also switches on automatically when PPO₂ is less than 0.19, and cannot switch off when unit is under pressure.

EN61508 requirements would demand handset switches on automatically when unit is used.

7.7 Oil Filled Chamber Leaks Oil

Cause

- Mechanical damage.
- Poor servicing or maintenance.
- Reservoir piston to accommodate thermal expansion is stuck.
- Reservoir for thermal expansion is too small.

Symptoms

Surface

- Filling oil visible inside unit.

Dive

- Smell of the filling oil inside the loop.
- If the pressure sensor is inside the oil-filled volume, it will show a lower (smaller) depth than is the actual depth.

Recovery action during Dive

- Bail out.

Preventative action

- Check unit for signs of leakage.

EN61508 Implication

HC sensor will detect leakage if the oil contains any hydrocarbons, but use of hydrocarbon filling oils is a dangerous practice and not recommended. Use of waxes (solid paraffins) causes serious problems with thermal expansion.

This failure could be detected using a differential pressure sensor, but this is an expensive solution that is prone to failure due to the thermal expansion of the oil.

Solution adopted by Open Revolution submission is to use food grade silicone oil to avoid a health hazard, and to remove all components liable to offgas from the oil-filled volume (moving them to a 1ATM compartment in the sea water). The remaining components then operate as if they are inside the breathing loop. This is then not a critical failure.

Consideration should be given to adding a perfume to the filling oil, so any leakage is apparent from the smell in the loop.

7.8 Electronic Component Explodes

Cause

- Use of inappropriate components.
- Failure becomes critical if component is not completely separated from the breathing loop.

Symptoms**Surface**

Odour inside breathing loop.

Dive

One-off noise.

Odour inside breathing loop.

Recovery action during Dive

Bail out.

Preventative action

Eliminate risk by design.

EN61508 Implication

Perform full self-test on power up.

Eliminate all components liable to explode (tantalum or electrolytic capacitors, all components incorporating a gel or a gas, all components incorporating an electrolyte).

Components that cannot be eliminated, such as the batteries, to be moved to a 1 ATM environment outside the rebreather, that can physically withstand the pressure rise from the component being vapourised. That is, the 1 ATM environment should withstand the vapour pressure from boiling off the electrolyte.

7.9 User unaware of failure message or unable to act

Cause

User should not understand the warning.

User is injured and not able to actuate unit, e.g. CNS toxicity.

User is entrapped by netting or cable limiting mobility.

Failure of back light on handset where user relies totally on the handset and is using the handset in a dark environment.

Failure of voice annunciation system where user relies totally on the voice annunciation.

Failure of buzzer, where user relies totally on buzzer.

Failure of Head Up Display.

Recovery action during Dive

Read the warning message, using a torch if necessary.

Preventative action

Proper maintenance and training.

EN61508 Implication

Provide a reference: in the Open Revolution submission this is the text display under the main handset display. This displays the failure and the action required. If in doubt the user can look to this display and receive succinct instruction on how to correct the problem, and its significance.

Provide multiple annunciation: the four above are included in the sports rebreather configuration - in the commercial diving configuration the handset functions move to a topside console.

Provide an automatic bail-out valve so user cannot ignore critical actions.

7.10 Faulty Software

Cause

Design not compliant with EN61508.

Symptoms

Surface

Any software malfunction.

Dive

Any software malfunction.

Recovery action during Dive

Bail out.

Preventative action

Ensure design meets EN61508.

EN61508 Implication

The industry is using software where nothing is verified, and even normal practices for non-safety-related software, such as automated GUI checks, are not applied.

No software or hardware control meeting EN61508 should encounter these issues at a safety critical level. The software should be formally verified.

7.11 Handsets Misread

Cause

Poor visibility in halocline or thermocline, with small font-size on handsets.

Lack of back light.

Symptoms

Surface

Error in reading handset.

Dive

Error in reading critical information on handset.

Recovery action during Dive

Check handset more carefully.

Preventative action

Check handset carefully.

EN61508 Implication

The main handset should have the largest display which it is practical to carry.

Large displays carry an increased risk of damage due to being dropped or mishandled. Suitable materials should be chosen to minimise this risk.

Displays must be backlit.

7.12 Cracked Electronics Housing

Cause

Housing subject to excessive mechanical stress, before dive or from pressure.

Inappropriate materials or stresses in handset design.

Symptoms**Surface**

Electronics malfunction.

Dive

Any electronics malfunction.

Recovery action during Dive

Bail out.

Preventative action

Service correctly and pre-dive checks.

EN61508 Implication

This problem occurs with electronics, particularly handsets that are not EN61508 compliant.

If the handset has two sets of electronics, then a failure of any one part should not cause failure of the whole. This is a natural product of any design meeting SIL 4.

The electronics should perform a JTAG test on start-up: this would identify the problem prior to dive.

7.13 Corroded wiring

Cause

Caustic cocktail.

Unit left in flooded condition.

No, or inadequate, conformal coating to wiring.

Symptoms

Surface

Electronics malfunction. Visible corrosion.

Dive

Any electronics malfunction.

Recovery action during Dive

Bail out.

Preventative action

Service correctly and pre-dive checks.

EN61508 Implication

This problem occurs with electronics that are not EN61508 compliant.

The electronics should perform a JTAG test on start-up: this would identify the problem prior to dive.

8 OXYGEN SENSOR FAILURES

8.1 O2 Cell Decompression Failure

Cause

Differential pressure on O2 cell.

Rapid decompression.

Rupture of rear membrane inside O2 Cell causes KOH to be deposited on to temperature compensation board.

Symptoms**Surface**

Not apparent.

Dive

If the diver flushes the loop, the PPO2 will be different from that expected.

Recovery action during Dive

Bail out.

Preventative action

Careful inspection of sensors. It is unreasonable to expect the user to do this on every dive.

EN61508 Implication

This is a serious failure in that it causes the O2 Cell reading to fluctuate both high and low depending on temperature.

Solution adopted is to change the sensor design to allow this problem to be detected. The temperature compensation circuit is removed and

replaced with a 1000ohm load. The electronics check for the existence of the 1000ohm load to verify that the correct sensor type is fitted and the load is there. Only then will it use that sensor reading (otherwise it will report a faulty sensor). This eliminates the problem at source.

8.2 O2 Cell has CO2 Contamination

Cause

High level of CO2, such as from pre-breathing without a scrubber, causes CO2 to migrate across O2 cell membrane, into KOH, where it converts KOH into water.

Symptoms

Surface

Not apparent.

Dive

If the diver flushes the loop, the PPO2 will be different from that expected.

Recovery action during Dive

Bail out.

Preventative action

If CO2 level high on start-up, check cells for droop.

EN61508 Implication

This is a serious failure in that it causes all O2 Cell readings to read low. This should be detected automatically by doing the O2 flush under start-up sequence control, and hence eliminated. O2 Cells need to be characterised for degree of droop in CO2.

8.3 O2 Cell Contamination

Cause

Organic material in O2 Cell KOH solution.

Symptoms

Surface

Drift of O2 Cell readings

Dive

May manifest as a ceiling fault during the dive.

Recovery action during Dive

Eliminate the sensor from the PPO2 calculation.

Preventative action

Check sensors for drift. Replace sensors that drift.

EN61508 Implication

Requires that the system check for need for sensor replacement and for sensor drift during successive calibration cycles.

8.4 O2 Cell Thermal compensation failure

Cause

Manufacturing fault, or component failure in O2 cell.

Symptoms**Surface**

Not apparent.

Dive

If the diver flushes the loop, the PPO2 will be different from that expected.

Recovery action during Dive

Bail out.

Preventative action

Careful inspection of sensors. It is unreasonable to expect the user to do this on every dive.

EN61508 Implication

This is a serious failure in that it causes the O2 Cell reading to fluctuate both high and low depending on temperature.

Solution adopted is to change the sensor design to allow this problem to be detected. The temperature compensation circuit is removed and replaced with a 100Ohm load. The electronics check for the existence of the 100Ohm load to verify that the correct sensor type is fitted and the load is there. Only then will it use that sensor reading (otherwise it will report a faulty sensor). This eliminates the problem at source.

8.5 O2 Cell Loose Connection

Cause

Corrosion or poor maintenance.

Symptoms**Surface**

Intermittent "Out of Range" or "Failure" messages on a cell. Failure to calibrate.

Dive

Intermittent "Out of Range" or "Failure" messages on a cell.

Recovery action during Dive

Diluent flush to check other 2 sensors respond correctly. Consider bail out. Abandon dive.

Preventative action

Service carefully.

EN61508 Implication

Use an SMB connector to minimise risk, by having a connector with multiple contact faces.

8.6 O2 Single Cell Failure

Cause

Exhausted or out-of-date cell. Cell internal failure.

Symptoms**Surface**

Intermittent "Out of Range" or "Failure" messages on a cell. Failure to calibrate.

Dive

Intermittent "Out of Range" or "Failure" messages on a cell.

Recovery action during Dive

Diluent flush to check which sensors respond correctly. Consider bail-out. Abandon dive.

Preventative action

Replace cells at correct intervals (every 12 months).

EN61508 Implication

Withstand multiple cell failures.

Engineer the cells so all failures are in the same direction (low).

8.7 O2 Two Cell Failure

Cause

Exhausted or out-of-date cells. Insufficient ions to produce voltages representing high O2 above set point.

Sensors exposed to CO2 following scrubber breakthrough.

Symptoms**Surface**

Intermittent "Out of Range" messages on a SINGLE cell (the good one). Failure to calibrate.

Dive

Intermittent "Out of Range" messages on a SINGLE cell (the good one).
Failure to calibrate.

EN61508 Implication

PPO2 controller must withstand multiple cell failures.

Engineer the cells so all failures are in the same direction (low).

Test the sensor ceiling by applying a higher load, while the sensor is in pure O2 during pre-dive checks. For example, if normal load internal to the sensor is 100 Ohms, then apply 50 Ohms to check ceiling is not lower than a PPO2 of 2.0.

8.8 O2 Cell Failures Tracked Incorrectly

Cause

Multiple O2 Cell failures with voting logic.

Preventative action

Do not use voting logic.

EN61508 Implication

Eliminate problem by carrying out a fault assessment of O2 Cell failure modes, then test of O2 Cells to a Test Plan to verify those modes.

Use sensor fusion algorithm that can detect one good sensor among faulty sensors.

Provide means to check sensors automatically when a sensor failure occurs, such as injecting a known quantity of O2. This requires a calibrated O2 injector: this can be done automatically during pre-dive checks.

8.9 O2 Cell Calibration Incorrect

Cause

User error and design omission, allowed the user to calibrate the CCR as if it was 98% O2, when PPO2 level in the loop could have been as low as 48%. Result was Cat III DCI.

Preventative action

All O2 Cells should calibrate in air when the unit is open: users should not be asked to calibrate with a gas supply which may not in itself be calibrated, injecting an uncalibrated amount of gas into an uncalibrated loop volume (the procedure used by the manufacturer).

EN61508 Implication

Eliminate problem by calibrating on air.

8.10 O2 Cells show different reading to independent PPO2 monitor

Diluent flush to check which sensors respond correctly. Bail out.
Abandon dive. Unit will maintain O2 limits on the 2 bad cells as they out-vote the good one. O2 will be high.

Preventative action

Replace cells at correct intervals (every 12 months). At start of dive, drive cells above set point to ensure they can respond fully.

EN61508 Implication

Withstand multiple cell failures.

Engineer the cells so all failures are in the same direction (low).

8.11 O2 Cells have condensation on sensor face

Cause

Moist, warm, saturated gas, condensing on objects in the gas flow.

Symptoms**Surface**

Normally none.

Dive

Intermittent "Out of Range" or "Failure" messages on a cell.

Recovery action during Dive

Diluent flush to check which sensors respond correctly. Bail out.
Abandon dive.

Preventative action

Latest cells have face which is hydrophobic. Insulate loop to lower condensation.

EN61508 Implication

Withstand multiple cell failures.

Important issue is to ensure calibration is not carried out in cells with water on their faces. This is an issue if the calibration is performed while fitting a new scrubber. The calibration should be performed after the scrubber is closed.

The training manual should emphasise the checking of the unit by a DIL flush.

8.12 O2 Cells have differential pressure applied

Cause

Unequal pressure on front and back of sensor cells during dive.

Symptoms**Surface**

None.

Dive

Intermittent "Out of Range" or "Failure" messages on a cell.

Recovery action during Dive

Diluent flush to check which sensors respond correctly. Bail out.
Abandon dive.

Preventative action

Ensure gas flow to rear of cells. Make sure pressure equalisation holes are clear, and that the sensor pcb has equalisation holes.

EN61508 Implication

Withstand multiple cell failures.

Ensure the design allows adequate gas flow to rear of cells to eliminate the source of failure.

Engineer the cells so all failures are in the same direction (low).

8.13 O2 Cell Explodes

Cause

Lockout of an O2 Cell in a chamber.

Symptoms

Surface

Shrapnel injury to operator. Strong alkaline spray (KOH).

Dive

Not applicable.

Recovery action during Dive

Not applicable.

Preventative action

Do not decompress O2 Cells faster than a human can withstand.

EN61508 Implication

Verify that sensors specified for product do not produce shrapnel when suddenly decompressed (Torpedo test).

Warn operators that if an O2 Cell feels wet, they should wash the sensor and hands in warm water immediately. Requires note in training manual.

9 DIVER FAILURES

9.1 Breathing off loop that cannot sustain life

Cause

User fails to bail out.

Frequent cause of fatalities on CCRs.

Symptoms

Surface

Any warning ignored.

Dive

Any warning ignored.

Recovery action during Dive

Bail out.

Preventative action

Force bail-out automatically if user should not act on warnings.

EN61508 Implication

Implement a fail-safe automatic shut off valve; bail-out is essential.

10 CO2 RELATED FAILURES

10.1 Scrubber Not Fitted

Cause

User error.

Symptoms

Surface

Rapid breathing, headache. Hypercapnia.

Dive

Stiffness, rapid breathing, confusion.
Hypercapnia.

Recovery action during Dive

Bail out.

Preventative action

Provide monitoring to check presence of scrubber.

EN61508 Implication

Monitor scrubber health.

Monitor scrubber life.

Monitor when the scrubber is changed.

Monitor PPCO₂.

Measure breathing resistance across scrubber, to detect this failure automatically.

10.2 Scrubber Physically Damaged, affecting gas X-section

Cause

Poor handling, with poor user check when installing scrubber.

Symptoms

Surface

Rapid breathing, headache. Hypercapnia.

Dive

Stiffness, rapid breathing, confusion. Hypercapnia.

Recovery action during Dive

Bail out.

Preventative action

Check scrubber visually before installation. If granular scrubber, weigh the scrubber.

EN61508 Implication

Provide monitoring to check for pressure across scrubber when user opens mouthpiece after positive pressure test. Absolute pressure records drop over time, and max pressure in loop, so differential pressure across scrubber varies only as a function of poor scrubber packing, fitting or damage.

10.3 Scrubber Exhausted

Cause

Overuse or improper storage. Out of date.

Symptoms

Surface

Rapid breathing, headache. Hypercapnia.

Dive

Stiffness, rapid breathing, confusion. Hypercapnia.

Recovery action during Dive

Bail out.

Preventative action

Change the scrubber every 3 hours or sooner.

EN61508 Implication

Monitor scrubber health.

Monitor scrubber life.

Monitor when the scrubber is changed.

Monitor PPCO₂.

10.4 Scrubber Bypass

Cause

Gas flows rapidly through a single path in the scrubber and CO₂ is not removed.

Bad packing. Material published by APD indicates that a large proportion of their user base cannot pack a granular scrubber properly to prevent this problem.

The most popular axial scrubbers have an endemic by-pass of 0.1 to 0.2% CO₂ due to poor scrubber design. This means the scrubber must be tested flat in these designs.

Symptoms

Surface

Rapid breathing, headache. Hypercapnia.

Dive

Stiffness, rapid breathing, confusion.
Hypercapnia.

Recovery action during Dive

Bail out

Preventative action

Design-out the problem by using an EAC.

EN61508 Implication

Monitor scrubber health.

Monitor scrubber life.

Monitor when the scrubber is changed.

Monitor PPCO₂.

Granular material packed by users will not meet EN61508 at any SIL level.

Design-out the problem using an EAC.

10.5 Excess Work of Breathing

Cause

Diving to excess depth for the rebreather.

Use of filter or skrim material to prevent caustic dust.

Overpacking of scrubber.

Moisture absorbed by scrubber during use increases breathing resistance and hence WOB.

Flooding.

Mushroom valve stuck shut.

Counterlungs change position.

Preventative action

Measure WOB actively during dive.

10.6 Counterlungs change position, causing CO2 hit

Cause

Possibility to put on rebreather without counterlungs being fixed down.

Symptoms

Surface

Not noticeable.

Dive

Increased WOB leading to severe CO2 hit.

Recovery action during Dive

Bail out on to open circuit.

Preventative action

Service correctly and pre-dive checks.

EN61508 Implication

Counterlungs should be fixed down so that user cannot disconnect one end, or fail to attach counterlungs.

10.7 One Way Valve Stuck Open

Cause

Valve not fitted.

Valve stuck open due to debris in the valve, particularly following a flood or vomiting into the loop.

Some valve designs allow them to jam open.

Incorrect assembly: mushroom is inserted on to the wrong side of the spider.

The wrong mushroom is inserted to the wrong side of the mouthpiece.

Symptoms

Surface

Same as scrubber breakthrough.

An attentive diver may notice the breathing bags moving in a different sequence to normal.

Dive

Same as scrubber breakthrough.

Recovery action during Dive

Bail out.

Preventative action

Pre-dive check for valve operation.

EN61508 Implication

The function of the two one-way valves fitted either side of the mouthpiece is critical to the safe operation of the unit.

The design must be of a type that shall not stick by itself. The Open Revolution design conforms with this requirement: it is a silicone mushroom valve, with no springs or other elements.

The mushrooms must be colour-coded and of a different design on each side, so the exhale mushroom cannot be inserted to the inhale valve, and vice versa.

The spider supporting the mushroom should have pegs to prevent the mushroom being assembled on to the wrong side of the spider.

The two spiders should be of different size, or keyed, to prevent the inhale valve being inserted in the place of the exhale valve.

10.8 One Way Valve Stuck Shut

Cause

Valve stuck shut due to sticky material on the valve, particularly following a flood or vomiting into the loop.

Some valve designs are prone to jam shut.

Incorrect assembly: mushroom is inserted onto the wrong side of the spider.

The wrong mushroom is inserted to the wrong side of the mouthpiece.

Symptoms**Surface**

Diver sees a very high breathing resistance.

Dive

Same as on surface. It should be obvious what has occurred on the surface.

Recovery action during Dive

Bail out.

Preventative action

Pre-dive check for valve operation.

EN61508 Implication

This is a fail-safe failure: the unit cannot be breathed because the breathing resistance is too high. This problem shows up during pre-dive checks.

11 OTHER FAILURES

11.1 Allergic Reaction to Material

Cause

Use of latex or other allergenic material.
Foreign matter in loop, especially mouthpiece, such as from jelly fish.

Symptoms**Surface**

Can vary from difficulty breathing, burning around mouth through to toxic shock.

Dive

Same as on surface.

Recovery action during Dive

Bail out

Preventative action

Use a full-face mask.

EN61508 Implication

Eliminate all allergenic materials from loop.

11.2 BC Failure

Cause

Puncture or structural failure of BC.

Symptoms**Surface**

Unable to inflate.

Dive

Unable to inflate.

Recovery action during Dive

Abandon dive. Use alternative buoyancy source. Ditch weight belt if necessary.

Preventative action

Service regularly and test/inspect.

EN61508 Implication

Outside eCCR, but covered in “end to end” clause.
Do not sell BC with eCCR.
Use redundant BC, such as OMS twin bladder BC.

11.3 Harness Failure

Cause

Structural failure of component.

Symptoms

Surface

Back unit swings and becomes loose.

Dive

Unlikely as unit’s weight is water-supported.

Recovery action during Dive

Tighten other straps. Abandon dive if unable to re-secure.

Preventative action

Service regularly and test/inspect.

EN61508 Implication

Use multiple attachment points.

11.4 Loop Flood

Cause

Puncture or structural failure in the loop.
Hoses from EPDM do not split, but develop small holes.
Hoses can separate from their couplings.
Breathing bag could fail catastrophically due to seam failure.
Connectors may not be installed correctly.
Connectors have inadequate keying, particularly where these penetrate the scrubber canister.

Symptoms

Surface

Pre-dive check failure. Unable to hold set point.

Dive

Gurgling and other signs of water in loop. Breathing resistance.

Recovery action during Dive

Bail out.

Preventative action

Protect hoses with covers and service regularly. Pre-dive checks.

EN61508 Implication

Monitor moisture and WOB. Warn user of flood and give instructions to bail out.

Design-out risk of connectors not being installed correctly by using very positive identification and colouring to show how far the connector should be installed.

Double-weld the breathing bag, using RF welding.

Hoses should be made from EPDM. It may be better not to have a wrap over the hoses, so damage is more immediately apparent. Survey of hose leakage on Rebreather World confirms hoses of thick EPDM construction fail with small leaks before any major leak occurs. This is not true of thin-walled hoses.

Eliminate all failure points into scrubber by providing full hose connector as an integral part of the scrubber canister, rather than using keyed or bonded elements.

11.5 Pressure Sensor Failure.

Cause

Any pressure sensor failure (gas contents, ambient, differential).

Recovery action during Dive

Abort dive.

Preventative action

Monitor pressure monitors frequently.

EN61508 Implication

The failure modes of the pressure sensors should be determined, and failure actively detected. The appropriate warning can then be raised.

11.6 Gross dry suit leak

Cause

Poor maintenance.

Zipper failure.

Ripped suit material.

Preventative action

Check dry suit carefully before use.

Handle zippers carefully.

Use proper maintenance and inspection.

EN61508 Implication

Covered by “end to end” clause.

Provide active suit heating using self-regulating carbon monomers to maintain the thermal balance for 30 minutes (max time for diver to return to bell).

11.7 Counter-diffusion hazard

Cause

Use of breathing gases with END less than 0msw.
Use of different gases between suit and breathing loop.
Switching between gases with different constituents.

Preventative action

Training on hazards of counter diffusion.

EN61508 Implication

Measure N2 by deduction of other gases, and give alarm if less than 500mbar of N2.
State hazard clearly in training manuals.

11.8 Noxious chemical off-gassing

Cause

Unsuitable materials in breathing loop.
Contamination of breathing loop.

Preventative action

Check all plastic materials and coatings used in breathing loop for health hazards, by appropriate searches and MSDS checks.

EN61508 Implication

No PTFE or PVC. Avoid complex plastics.

11.9 Vomiting into breathing loop

Cause

Contaminated breathing gas.
Sea sickness.
Alcohol, drugs or ill health.

Preventative action

Use certified breathing gas.
Do not dive under influence of alcohol or drugs.
Do not dive in case of bad health.
Maintain an O.C. regulator to be sick through.

EN61508 Implication

It is beneficial to have an O.C. regulator in the system. This would require a breathable gas at all times.

Requires breathing hose of sufficient diameter so as not to be blocked by vomit. Experiments using frozen carrots and sweetcorn in yoghurt (40%,30%,30%) indicate that a 36mm diameter hose and fitting is required.

11.10 Deco dive with incorrect PPO2 level in loop

Cause

User error and design omission allowed the user to calibrate the CCR as if it was 98% O₂, when PPO₂ level in the loop could have been as low as 48%. Result was Cat III DCI.

Preventative action

All O₂ Cells should calibrate in air when the unit is open: users should not be asked to calibrate with a gas supply which may not in itself be calibrated, injecting an uncalibrated amount of gas into an uncalibrated loop volume (the procedure used by the manufacturer).

EN61508 Implication

Eliminate problem by calibrating on air.

11.11 DCS risk higher than statistical projection of deco algorithm

Cause

Bugs in deco software.

Inherent risk of deco algorithm used.

Other health problem leading to predisposition to DCS.

Preventative action

All decompression software should be formally verified to prove that the algorithm implemented is actually that intended.

Full, regular health check-up.

EN61508 Implication

Verify the deco algorithm is implemented correctly using formal methods.

11.12 CNS Toxicity

Cause

- 1.Failure of PPO₂ controller (not meeting EN61508).
- 2.Serious PPO₂ spiking during descent.
- 3.Injecting O₂ instead of DIL.
- 4.Diver bailing out on to O₂ instead of on to DIL or off-board bailout.
- 5.Incorrect use of CNS calculation. Original papers describing CNS calculation are based on a 4% reduction in vital capacity with 100% CNS loading (Oxygen Toxicity Calculations. E. Baker). NUI research paper indicating 1% of users having CNS toxicity effects at 75% CNS loading. Despite this, users believe they can tolerate 100% CNS loading as a basic

plan: some report regular dive planning with 175% and 250% CNS loading.

Preventative action

CNS clock in common use has CNS convulsion incidents reported at as low as 25% CNS loading.

Original paper on CNS measures loss of lung surficant as primary measure of CNS damage, with 1% at 75% CNS clock and 4% at 100%. Use less CNS clock.

EN61508 Implication

Modified CNS algorithm, with margin to reduce statistical incidence of measurable CNS damage. Published on DL Web Site, and on Rebreather World, with formal model to enable implementation to be verified.

CCR controller should track CNS and maintain within safe limit, by adjusting PPO2 set point if necessary.

Provide a Chicken Switch for the commercial diver using a helmet, as loss of speech is one of the first indicators of CNS (from interviews with CNS tox victims).

There should be no measurable loss of lung surficant during a dive. This requires downrating the CNS clock as above.

This is a critical failure that has caused more than one death.

Eliminate all scirms in the design.

Eliminate scrubber packing variance.

Use EAC scrubber to eliminate change in breathing resistance during use.

Measure WOB actively pre-dive and during the dive, and warn user.

Measure respiratory parameters and warn the user when these move outside normal or safe ranges.

12 FAILURES SPECIFIC TO SURFACE-SUPPLIED DIVES

12.1 Loss of Umbilical (Commercial diver)

Cause

Disconnection.

Heavy object falling on umbilical.

Cutting of umbilical.

Failure of topside to provide umbilical support.

Preventative action

Reduce umbilical services to the minimum: power, communications and umbilical gas feed.

EN61508 Implication

Must be survivable by use of bail-out carried by diver. Maximum depth and maximum O2 concentration in bail-out gas determines bail-out size.

12.2 Cut of umbilical near surface (Commercial Diver)

Cause

Disconnection.
Heavy object falling on umbilical top-side.
Cutting of umbilical.
Failure of topside to provide umbilical support.

Preventative action

Risk is the diver being sucked into the umbilical due to the pressure in the umbilical being much less than the ambient. Fit a one-way valve to the umbilical at the point where it feeds into the diver's helmet.

EN61508 Implication

One-way valve is required.
Adequate bail-out is required. Must be survivable by use of bail-out carried by diver. Maximum depth and maximum O₂ concentration in bail-out gas determines bail-out size.

12.3 Entrapment of Umbilical (Commercial diver)

Cause

Heavy object falling on umbilical.

Preventative action

Reduce umbilical services to the minimum: power, communications and umbilical gas feed so it can be moved more easily.
Diver should be trained to safeguard umbilical.

EN61508 Implication

Umbilical must be either disconnectable or the diver must carry means to cut the umbilical to free himself.
CNC Toxicity (Commercial Diver).

12.4 Loss of Helmet (Commercial diver)

Cause

Inadequate attachment.

Preventative action

Use helmet that requires at least two actions using two hands to detach.

EN61508 Implication

Entire helmet comes within EN61508 by virtue of it containing electronic functions (microphone etc).
Monitor electronically whether a helmet is attached correctly.
Require at least two operations using two hands to detach helmet.

12.5 Sudden change in depth (Commercial diver)

Cause

Falling into a hole, or uncontrolled rise, causing intermediate pressure from umbilical gas to be either excessive or insufficient.

Preventative action

System should bleed off excess umbilical pressure.
One-way valve needed in case of negative pressure.

EN61508 Implication

Same as for umbilical being cut near surface.

12.6 CO in loop (Commercial diver)

Cause

Contaminated breathing gas.
Metabolism product.

Preventative action

Flush loop periodically, and test for CO.

EN61508 Implication

Requires active CO monitoring on the diver.

12.7 HC or Volatile Organic Compounds in Loop (Commercial diver)

Cause

Contaminated breathing gas.
Metabolism product.
Off-gasing of plastics or cleaning agents in rebreather.

Preventative action

Flush loop periodically, and test for VOCs.

EN61508 Implication

Requires active HC and VOC monitoring on the diver.

12.8 Loss of communications (Commercial Diver)

Cause

Equipment failure.
Inattentive operator.
Collision on surface.
Failure of umbilical link.

Preventative action

Use multiple communication paths.

EN61508 Implication

Requires at least two communication paths.
 Provide communications to bell in addition to comms to surface.
 Question on through-water ultrasonic comms.

12.9 Loss of Suit Heating (Commercial diver)**Cause**

Electrical failure.

Preventative action

Use sufficient passive thermal protection to return to the bell.

EN61508 Implication

State requirement for passive undersuit thermal protection in user manuals and training.

12.10 Excess suit heating (Commercial diver)**Cause**

Electrical failure.
 Top-side operator error.

Preventative action

Eliminate by use of self-regulating materials.

EN61508 Implication

Eliminate failure mode by use of self-regulating materials, and use of active current monitoring to detect shorts or excess current drain.

13 GENERAL DIVING HAZARDS

Sports diving in general seems to have a risk of accident of between one in 10,000 hours to one in 100,000 hours, depending on the type of diving being carried out [3], [4]. Some of these accidents are due to equipment failure [6], most are due to lack of training, lack of attention, poor judgement or the effect of an underlying illness or predisposition. Use of rebreathers has considerably higher risks based on the same accident figures and the population of rebreather divers. The increase appears to be associated with failures to meet EN61508 in the equipment design: the rebreathers with the shortest MTBCF have the highest rates of fatal accidents, and rebreathers with the best MTBCFs have the lowest rate of fatal accidents.

Commercial diving seems to have a significantly lower accident rate than sport diving, based on IMCA accident reports [5] and the amount of commercial diving carried out. Commercial diving has had a much larger amount of research carried out into the health and safety of divers than is the case for sports divers.

All diving carries some short and long term risks to health.

Long-term risks are described by D.H. Elliott & R.E. Moon [1]. All long-term health risks appear to originate from an event that can also give rise to a short-term risk, such as an

untreated DCS or barotrauma. In some cases the long-term risk is due to a succession of minor insults, in other cases, from the effect of cellular damage from a single insult which may, at the time, have appeared insignificant.

Short-term risks are compiled from D.H. Elliott & P.B. Bennet [2], DAN and BSAC accident reports, as follows:

Health Risk	Cause and effects
Respiratory Gases	<p>Contaminated breathing gas, with effect of narcosis, anaesthesia, illness.</p> <p>Unsuitable breathing gas for depth: hypoxic or hyperoxic, with effect of loss of consciousness, convulsions</p> <p>Narcotic breathing gas with effect of loss of judgement, time perception, consciousness.</p> <p>Insufficient gas, with effect of drowning.</p> <p>Gas switch between gases with large difference in anaesthetic effect, with effect of loss of consciousness.</p> <p>Counter-diffusion with effect of DCI.</p>
Diving Reflex and Sudden Death Syndrome	<p>Water contact on forehead has effect of "Whale Diving Reflex", with constriction of blood vessels, slowing of heart beat and increase in blood pressure. Implicated in Sudden Death Syndrome in older divers.</p>
Thermal Balance	<p>Lack of thermal protection, with effect of hypothermia or aborted dive with decompression load.</p> <p>Suit leaks without means to heat the suit cause hypothermia.</p>
Exhaustion	<p>Swimming against strong current, effect of loss of energy to remain afloat.</p>
Loss of Buoyancy Control	<p>Loss of buoyancy control with effect of uncontrolled ascent or descent.</p> <p>Entanglement in surface towed objects with effect of loss of buoyancy control, causing DCS, barotrauma or drowning.</p> <p>Entanglement with object moving towards surface, such as a lift bag or SMB reel, with effect of loss of buoyancy control, causing DCS, barotrauma or drowning.</p>

	<p>On surface, diver fails to drop weight belt when in difficulty, with effect of drowning.</p> <p>Failure of BC valves with effect of uncontrolled ascent or descent.</p> <p>Confusion by diver causing diver to press inflate button when intends to deflate, or vice versa, with effect of uncontrolled ascent or descent.</p> <p>Weight jackets may redistribute weight, causing diver to be “up-ended”, with effect of drowning. Simple weight belts should be encouraged, with retainer to prevent accidental loss.</p> <p>Loss of control of dry-suit gas may cause diver to be “up-ended”, which, without training, the diver may not recover from. Recovery method is simply to form a ball and roll out. If diver does not succeed, then effect may be drowning.</p>
Disorientation	Illness, vertigo, reduction in visibility, unfamiliar environment with effect of panic or behaviour leading to entrapment or becoming separated underwater. Ultimately effect may progress to drowning from insufficient respiratory gas, or barotrauma from loss of buoyancy.
Perceptual Narrowing	Stress, leading to information essential for safety being ignored.
Panic	Predisposition, asthma, lack of training, with effect of excess use of respiratory gas, behaviour contrary to safety.
Barotrauma	<p>Breath-holding during ascent, from as little as 1.2m, with effect of gas embolism.</p> <p>Loss of buoyancy leading to pulmonary barotrauma, alternobaric vertigo, compression barotrauma, or any embolism.</p> <p>Illness causing gas blockage, with effect of embolism on lungs.</p> <p>Prostheses or dental cavity, with effect of acute pain.</p>
DCS	As per CCR hazards.
Dehydration	Serious sea-sickness, or alcohol abuse, drugs, poor hydration practice, with effect of increased

	DCS risk and may have effect of loss of consciousness in extreme cases.
Heart Attack or Stroke induced by unaccustomed exercise	May be induced by Dive Reflex. Effect is invariably drowning.
Unconsciousness	Asthma, epileptic fit, insufficient or unsuitable respiratory gas, oxygen convulsion, CO2 retention, illness, generally with effect of drowning.
Underwater explosions	Proximity to naval exercises, or commercial demolition. Effect is pulmonary and intestinal rupture and haemorrhaging.
Underwater electric current	Commercial operations, leading to involuntary spasm and likely drowning.
Venomous marine life	Contact with any venomous sea life, particularly jelly fish, stonefish, some octopus, sea snakes, conch shells, parasites. Effect: shock, pain, nerve damage, or in case of parasites, damage to internal organs or brain.
Predators	Rare, with bites from large sharks, rays, squid, eels, seals.
Hard impacts	Impact with boats, propellers, divers falling on divers below, on to rocks in surf or heavy waves, with effect of trauma.
Excess Mechanical Shock or Strain to bone	Carrying heavy objects, with effect of bone fracture, breakage, or arthritis, osteonecrosis, muscle strain.

REFERENCES:

- 1.D.H. Elliott & R.E. Moon, "Long Term Health Effects of Diving", Ch21, pp585-604 of The Physiology and Medicine of Diving, P. Bennett & D. Elliott, 4th Edition.
- 2.D.H. Elliott & P.B. Bennett, "Underwater Accidents", Ch9, pp238-252 of The Physiology and Medicine of Diving, P. Bennett & D. Elliott, 4th Edition.
- 3.DAN (Divers Alert Network) Reports available from <http://www.diversalertnetwork.org/>

4. British Sub Aqua Club Accident Reports, from <http://www.bsac.org/safety/index.html>
5. International Marine Contractors Association reports, from <http://www.imca-int.com/divisions/marine/publications/dpsi.html>
6. UK Health and Safety Laboratory Research Report 424, "Performance of Diving Equipment" by N. Bailey, J. Bolsover, C Parker and A Hughes, 2006
7. A. Deas, "How Rebreathers Kill People", available from <http://www.deeplife.co.uk>