How Rebreathers Kill People

Objective: To make using a rebreather no more dangerous than getting on a Boeing 737 shuttle from Edinburgh to London

July 2005

Oct 2005 Updated with Incident 13

July 2006 Updated with Incidents 14 to 20

Sept 2007 Updated with Incident 21 and comparison with O.C. safety

Sources of Safety Data

- Failure Mode Effect and Criticality Analysis (FMECA)
- Incident Reports:
  - Incidents Survived
  - Coroner´s Reports
  - Fully Documented Fatalities
  - DAN
  - Fatal accident investigations, with formal modelling of events to narrow the cause.

900 times more dangerous than O.C.

- DAN report that there are 80 to 100 fatal accidents per 500,000 to 1 million active divers in the USA, per year. Most divers use O.C.
- Rebreather divers are more experienced, more qualified and much less obese than average O.C. SCUBA divers. According to DAN figures, this should make them 8 times safer still, i.e. one death per 80,000 per year.
- There have been 83 fatal accidents on rebreathers from 1994 to September 2007, with an average of around 2500 active participants over that time, a fatal accident rate of one in 391 per year.
- This means that SCRs and CCRs together are 204 times more dangerous than Open Circuit.
- For eCCRs, the figure is 900 times higher than for Open Circuit.
- These statistics indicate that equipment choice has a dramatic effect on dive safety. Why?

FMECA Reports

- Requirement of EN14143 that manufacturers perform an FMECA
- No requirement to publish results
- All manufacturers are keeping their report confidential
- EN14143:2003 requires compliance with EN 61508, which in turn requires 1 billion hour fault tolerance, but is not implemented by manufacturers (CE Marks are being put on equipment falsely)

Users and Government Safety Organisations are turning a blind eye.

- Result is no existing rebreather can tolerate one worst case failure
- Result is users have not the faintest idea of the safety of what they are diving
- Result is no-one can challenge wrong conclusions in a FMECA
- Result is there is no FMECA data on which to built better systems

Recommendation: All manufacturers selling any piece of life critical equipment to the public should publish the full FMECA Report on their web site along with the EN 61508 calculation and safety case.

Some Example Incident Reports

Incidents 1 to 10 are from one dive club. Incidents 11 to 22 are from fatality or serious accident reports.

1. Computer decided to do a cal underwater, all on its own
2. Computer Hanging
3. Displaying wrong PPO2 values when all sensors are working
4. Sudden massive flood, including CO2 hit and caustic cocktail
5. All O2 sensors failed
6. Mistakenly injecting O2 on descent instead of diluent
7. Loss of diluent on descent
8. O2 injector sticks on
9. Connector mismated: flood
10. Manifold O ring fails
11. CO2 retention due to increase in Work of Breathing caused by fitting faulty component
12. CO2 hits due to scrubber failure
13. Unit not switched on
14. PPO2 falls below that required to sustain life due to slow O2 sensors
15. O2 injection rate insufficient for ascent: this is an error in EN14143:2003
16. PPO2 set point allowed to be lower than that required for safe ascent
17. Errors in O2 sensor calibration
18. Bugs in decompression software
19. CNS toxicity
20. Use of uncalibrated “O2”
21. Software error on restart underwater
22. Majority cell error

Incident 1: Jump to Cal

Location: Scapa Flow, May

Dive Profile: Diving to 100ft, displays showed PPO2 at set point of 1.3.

Incident Report: "I heard O2 injector come on and stayed on all of its own accord. Looked at handset. It had jumped to performing a calibration and was injecting pure O2. Bailed out. No alarms."

Cause: This eCCR was the market leader. Checks by qualified electronics engineer found:

- Controller was effectively a single unverified microcontroller, running unverified code, compiled using an unverified compiler, running in an incompetent electronic design
- Unused memory locations were random codes when they should have been a jump to a recovery point.
- There was no Watchdog Timer installed. This is absolutely essential.
- The Brown-Out Circuit was tested and design found to be completely ineffective.
- Power supply circuits were prone to brown out.
- Multiple software errors.

Manufacturer advised, corrected shortcomings on new product, but did not recall any product. These faults were not disclosed to coroners investigating deaths, in circumstances where the Coroner may have concluded the CCR controller was the cause if disclosure was made.

Recommendation: CE requirements need to be enforced: application of BS EN 14143:2003 and its requirement to meet BS EN 61508, would have prevented these deaths.

Incident 2: Hanging Computer

Location: Scapa Flow, June

Dive Profile: Diving to 110ft, displays showed PPO2 at set point of 1.3.

Incident Report: "It occurred to me that the O2 injector was not firing (it was silent for too long). Did a flush. Displays stayed the same. Did not respond to buttons. Concluded computer had hung. No alarms sounded.
Tried switching off and back on. Computer insisted on calibrating
sensors. On cal, computer injected pure O2 even though depth was 110ft.
Bailed out. If I had not been listening for the O2 injector, I would be dead."

Cause: System checked by qualified electronics engineer.

- Unused memory locations were random codes when they should have been a jump to a recovery point.
- There was no Watchdog Timer installed.
- The Brown-Out Circuit was tested and design found to be completely ineffective.
- Power supply circuits were prone to brown out.

Manufacturer advised, corrected shortcomings on new product, but did not recall any product

These faults were not disclosed to coroners investigating deaths, in circumstances where the Coroner may have concluded the CCR controller was the cause if disclosure was made.

Recommendation: CE requirements need to be enforced: application of BS EN 14143:2003 and its requirement to meet BS EN 61508, would have prevented these deaths.

Incident 3: PPO2 Falls

Location: Leith Dock, October

Dive Profile: Quayside

Incident Report: “When injector fires, display PPO2 drops due to current drain. Almost new batteries. System then keeps injector on for too long, so PPO2 level see-saws.”

Cause: Engineers from two companies each specialising in dive safety were present.

- Problem caused by lack of screening on O2 sensor cables and poor power supply circuit.

Manufacturer advised, investigated but declined to fix problem.

Recommendation: Publishing FMECA would have highlighted the problem.

Incident 4: Sudden Flood

Location: Lower Clyde, June

Dive Profile: Deep Support Diver for an extremely deep dive

Incident Report: "Sudden massive flood and CO2 hit. Caustic cocktail inhaled, lots of it. Difficult getting back to surface and staying on surface
due to loss of buoyancy because of flood. When CO2 hit, under influence of CO2 hit, caustic cocktail in mouth but hallucinated it was in nose.
No warning headache. Became a critical situation. Averted by last second bail out. Due to CO2 did not think of dropping my weight belt."

Forums and bulletin boards contain a number of similar reports.

Cause: Caused by inadequate keying of hose: unit passes pressure tests with hose rotated and not in keyed position, if hose nut is tightened down. However, a bump on the hose causes it to fail with water pouring into the scrubber. The hose keying is a serious design fault. Manufacturer advised, disregarded problem. Charged for service of rebreather, writing "Not dishwasher proof" on inside of scrubber lid after user completely stripped it down and tried a dishwasher to remove caked on caustic chemicals. Early warning of a flood (gurgle) not covered in course.

Recommendation: An FMECA should have highlighted the problem. This indicates that no adequate FMECA was carried out. The manufacturer has sinced changed their training procedure and manuals to highlight the effect of a flood.

Incident 5: Multiple O2 Sensors Fail

Location: Dunbar, August

Dive Profile: To 160ft, Beside Bass Rock

Incident Report: "One O2 sensor failed during dive (lower than others). Running on 2 sensors. Then injector was injecting more often than I would expect given constant depth. Flush indicated PPO2 was different to what I expected, but not massively. I made an error in this due to narcosis. Concluded (incorrectly) that O2 injector was firing more often due to blockage in O2 line. Aborted dive remaining on closed circuit. Twitches on lip developed during ascent, assumed (again incorrectly) to be a due to a jellyfish: there were a lot of Lion´s Mane about and one had touched my mask. During ascent suddenly injector firing problem cleared. Descending again caused injector problem to return. Remaining O2 sensors had both developed a ceiling fault at the same time. Based on depth and set-point at which injector was working normally (25ft, PPO2 of 1.2) I recognised this as a ceiling error on the other two cells."

Cause: Unsafe O2 injection algorithm: PPO2 was up to 3.0 at onset of problem! Replacement of all cells at the same time is a bad practice. Voting logic is prone to follow cell failures.

Recommendation:

- A fault tolerant PPO2 controller is mandated in Europe, but the law is not applied.
- Cells should not be replaced at the same time.
- CCRs should not use voting logic for O2 controllers to substitute for a properly designed sensor management subsystem.

Incident 6: Injecting O2 Accidentally

Location: Dunbar, September

Dive Profile: To 130ft, Beside Bass Rock

Incident Report: "Was very tired that day as I had had a lot of hassle. Still thinking about it during start of dive. Thought alarm was from another diver who had something bleeping (boat load going down together). Before I saw the bottom, felt very bad and left eye was twitching then left eye closed out (like seeing a curtain come down half way and what was left was in negative colour). Saw handset with other eye which was normal. PPO2 was showing over 2.1. Bailed out and simultaneous did max rate ascent to 20ft. Ascent so fast it was off scale of dive computer, a Cochran, which locked out afterwards. Then from 20ft slow ascent to surface. Took about 10 minutes for eye to return to normal."

Cause: User kept pressing O2 button instead of dil button on descent.

Recommendation:

- Would have been avoided if Auto Shut-Off valve fitted.
- Question on why O2 manual button is needed.
- Requires clearer alarms, such as voice annunciation.

Incident 7: Loss of Dil

Location: Dunbar, September

Dive Profile: To 60ft

Incident Report: “Dil injector came off during descent. Descent accelerated while trying to turn on bail out gas to bail out reg. Hit the bottom so hard it formed a mushroom cloud in the water. Fortunately only 60ft. Embarrassing minute. Had been concentrating on turning on bail out gas (switched off because I did not want freeflow on diving into the water), rather than filling the BCD which I should have done: when in a real squeeze, you get tunnel focus on breathing rather than depth.”

Cause: Dil connector not plugged in properly. No ADV fitted.

Recommendation: Suggested to manufacturer and to forums that an ADV be created. Many disagreed with need for ADV with connector that is not plug-in.

Incident 8: O2 Injector Stuck On

Location: Scapa Flow, April

Dive Profile: To 110ft

Incident Report: “O2 alarms went off. Injector was firing continuously.”

.

Cause:

- Injector stuck on, after first stage changed without changing interstage pressure.
- Solenoid Injectors fail too easily. Solenoid not designed for life critical systems.

Recommendation:

- Cheap solenoid injectors designed for machine automation should not be used for rebreathers as they are prone to rust and cannot tolerate the full range of intermediate pressures provided by dive first stage regulators in common use.
- The injector should be made from a rust free material, with reasonable oxygen compatibility, such as SS 6ML.
- The valve should be controlled by two solenoids, as they are in space systems, to address the problem of solenoid failure, and to ensure there is adequate power reserve available to operate the solenoid under fault conditions.

Incident 9: Connector Unplugs

Location: Scottish West Coast, May

Dive Profile: To 90ft

Incident Report: “Flood. After an earlier flood event, I had changed the original BCD to OMS 110lb dual wing, so no problem with buoyancy, so was able to do instant bail out with no buoyancy problems.”

Cause: Connector at the back of the unit: connector seals before it has positive ident. This allows unit to pass all negative and pressure tests with connector not properly engaged.

Recommendation: Where connectors are used in the breathing loop, they must not seal until locked.

Incident 10: Manifold Ring Fails

Location: Swimming Pool, Edinburgh

Dive Profile: To 12ft

Incident Report: “Lots of bubbles suddenly. Rotating around I could see it was from back of the unit. Manifold cap came loose. Just swam back on the surface. Rarely use the manifold. Removed it now permanently: it is completely unnecessary.”

.

Cause: Superfluous manifold, created additional failure points.

Recommendation: FMECA had failed to remove all non-essential points of failure.

Incident 11: WOB Failure

Location: Bushman´s Hole, South Africa

Dive Profile: To 900ft

Incident Report: See Report on Dave Shaw fatality on http://outside.away.com/outside/features/200508/dave-shaw-1.html and analysis of fault on http://www.rebreatherworld.com/showthread.php?t=1337&page=2&pp=10.

Cause: Fitting incorrect scrubber filter material.

Recommendation:

- Fit a Respiratory Monitor, so when respiratory rate becomes too high, or tidal volume too low, warn the user to breathe more deeply and slowly. Same monitor could detect increase in WOB at outset.
- Deep Life have a WOB monitor using the same hardware components as scrubber monitor. This means that adding a WOB monitor does not cost a cent more in terms of hardware build.
- Could be useful to fit a fan as an emergency assisted WOB, and this can double up as a breathing-bag-drier during battery recharge.

Incident 12: CO2 Hits

Location: Numerous reports, including fatality during 2nd Dive on HMS Dasher

Dive Profile: Occurs usually during decompression

Incident Reports: http://www.rebreatherworld.com and http://www.btinternet.com/~madmole/divemole.htm

Cause: Scrubber expires and no alarm.

Recommendations:

1. Fit a CO2 alarm
2. Fit an effective scrubber life monitor
3. Redesign the scrubber so it does not fail suddenly, but gradually, giving time for the alarm to sound and for the diver to take corrective action.

Incident 13: Unit not turned on

Location: Several deaths where the unit has been found to be switched off

Dive Profile: Not applicable

Incident Reports:

Cause: User error and design omission

Recommendations:

1. All eCCRs should turn on automatically when PPO2 is less than 0.20.
2. When the unit is switched on automatically, it is essential the design is one where it cannot hang under any possible circumstance. Therefore the user should never need to switch it off underwater.

Incident 14: PPO2 falls below that required to sustain life due to slow O2 sensors

Location: Found using formal verification tools checking O.R. design, reported on a dive forum, then users of existing rebreathers reported near fatal accidents due to use of slow sensors.

Dive Profile: Rapid ascent

Incident Reports:

Cause: User error and design limitation

Recommendations:

1. The sensors should be keyed so users cannot change the sensor type
2. The control software should check the rate of change of the sensors during cal and reject slow sensors. No existing CCR did this: it was possible to pass cal on all rebreathers that were checked, using sensors with 25 second response.
3. 9 of the 11 possible O2 sensor failure modes result in a low PPO2 reading or a slow sensor reading. The sensor voting algorithm can track this. The sensor processing should test for slow O2 response.
4. Use of an Auto Shut Off Valve safeguards the user in the event of this fault

Incident 15: O2 injection rate insufficient for ascent

Location: Found using formal verification tools checking O.R. design, then cross checked with existing rebreathers and found to correlate with high fatality rate on particular units

Dive Profile: Low PPO2 set point followed by rapid ascent.

Incident Reports:

Cause: Design limitation

Recommendations:

1. EN 14143:2003 needs a “work around” to comply with the standard while allowing the CCR to inject more than 6 litres per minute of O2 in emergency. One work around is to fit multiple injectors (as in the O.R. design).
2. Manufacturer must allow ascents up to 350ft/min (max possible with an inflated BCD), from the maximum depth and with the lowest PPO2 set point supported by the CCR.
3. Auto Shut Off Valve would have prevented the deaths caused by this fault.

Incident 16: PPO2 set point allowed to be lower than that required for safe ascent

Location: A distinct variant on Incident 15: Found again using formal verification tools checking O.R. design, then cross checked with existing rebreathers and found to correlate with high fatality rate on particular units

Dive Profile: Low PPO2 set point followed by rapid ascent.

Incident Reports:

Cause: Design error on particular rebreathers

Recommendations:

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

Incident 17: Errors in O2 sensor calibration

Location: Red Sea

Dive Profile: Deco dive

Incident Reports:

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.

Recommendations:

1. All O2 sensors 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).

Incident 18: Bugs in decompression software

Location: Multiple locations

Dive Profile: Deco dives

Incident Reports:

Cause: Failure to follow mandated design procedures

Recommendations:

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

Incident 19: CNS toxicity

Location: Multiple

Dive Profile: Long dives

Incident Reports:

http://www.rebreatherworld.com/rebreather-accidents-incidents/1632-o2-convulsion.html#post16022 and http://www.rebreatherworld.com/technical-rebreather-forum/4304-guide-about-setpoint-selection-deep-dives.html

Cause: Incorrect use of CNS calculation. Original papers describing CNS calculation is 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.

Recommendations:

1. Modified CNS algorithm, with margin to reduce statistical incidence of measurable CNS damage. Published on DL Web Site, and on RebreatherWorld, with formal model to enable implementation to be verified
2. CCR controller should track CNS and maintain within safe limit by adjusting PPO2 set point if necessary

Incident 20: Low FO2 in O2 Cylinder

Location: Singapore and UK

Dive Profile: Not applicable

Incident Reports: http://www.rebreatherworld.com/rebreather-accidents-incidents/5513-my-first-screw-up-boris-2.html and one

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.

Recommendations:

1. Rebreather itself should check the O2 composition before every dive. It has calibrated O2 sensors (if the recommendation to force calibration in air), and can inject O2 and check the composition of the loop gas on the surface to give an injector cal. It is not complex to compensate the injector cal for depth, such that no gas switch can introduce a low FO2 gas
2. Auto Shut Off Valve would have prevented the problem affecting the diver's safety
3. Voice annunciation of the resulting low PPO2 level would have prevented the problem affecting the diver's safety

Incident 21: Software Error

Location: Isle of Man, fatal accident, several others very similar

Dive Profile: To 11msw

Incident Reports: Detailed accident report available to authors

Cause: When unit is reset due to battery bounce, it does not re-enter dive mode automatically. Due to unit thinking it has a cell error, due to the high PPO2, it cannot enter dive mode.

Recommendations:

1. On reset, if the rebreather is under pressure or the diver is breathing (measured by the PPO2 falling), then the unit should immediately inject O2 to maintain a breathable gas in the breathing loop.

Incident 22: Cell Error

Location: Australia

Dive Profile: Under 40msw

Incident Reports: Fatal Accident. Detailed accident report available to authors

Cause: Unit did not require any regular factory service. User had not replaced O2 cells in 3 years. User was partially deaf and could not hear the buzzer.

Recommendations:

1. Units should lock out if not serviced annually, with a 3 month margin.
2. Units should test the O2 cells properly before a dive, automatically. This can be done within ALARP.

Other Reports

- No coordinated central body receiving information on rebreather deaths.

- Diver Mole is doing a good job for Inspiration, but list very incomplete, and sometimes puts down to user error what is equipment failure.

- For example, Ian Smith died almost certainly from Incident 2. The two divers resuscitated were hit by Incident 1.

- Too many reports simply cite “User Error”. Needs to be a change of attitude to: “Nobody dies on a rebreather from user error, unless they take the mouthpiece out of their mouth and do not replace it with something.”

- Diver Mole´s List of Inspiration Fatalities is: http://www.btinternet.com/%7Emadmole/DiverMole/DMDanger.htm#Mick

Preventing the Deaths

1. Rebreathers currently are nowhere near the standard expected of other life critical systems.
2. Most manufacturers have no staff with formal training in the design of life critical systems.
3. Open review and fitting better safety systems could have prevented all of the incidents reported here.
4. Technologies are available that would have prevented every one of the incidents cited here.
5. There is overwhelming evidence that people are dying because equipment is designed badly, with inadequate safeguards.