

One Set of Solutions to the CCR Safety Problem

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

July 2005

Solutions for eCCR Safety

- ✓ Built on a Solid Foundation: will never “hang”
- ✓ Fault Tolerant Architecture, giving > 1 billion hours MTBCF
- ✓ Safe PPO2 Control
- ✓ Effective Scrubber Monitoring
- ✓ PPCO2 Monitoring
- ✓ Full Gas Monitor
- ✓ Combined Auto shut-off, dil, bail-out and flush
- ✓ Voice Annunciation of Faults and Recommended Action
- ✓ Full Respiratory Monitoring, assist and bag drier
- ✓ Automatic Pre-dive Checks and Self Test
- ✓ Correct O2 calibration
- ✓ Save the Loony: expect users to have the odd bad day

The Manufacturing Cost of Safety

- Making the foundation solid, costs \$60 per unit
- Full fault tolerance costs \$70 per unit
- Safe O2 injection costs \$20 per unit
- Effective Scrubber monitoring costs \$70 per unit, due mostly to the flow sensors
- Full gas sensing costs \$17 per unit
- CO2 Sensing costs \$180 per unit
- Auto-ShuDBoF Valve costs \$55 per unit
- Voice annunciation costs \$8 per unit
- Safe O2 calibration costs \$3 per unit
- Full self test and checks cost \$0.20 per unit
- Idiot tolerant control, costs nothing per unit

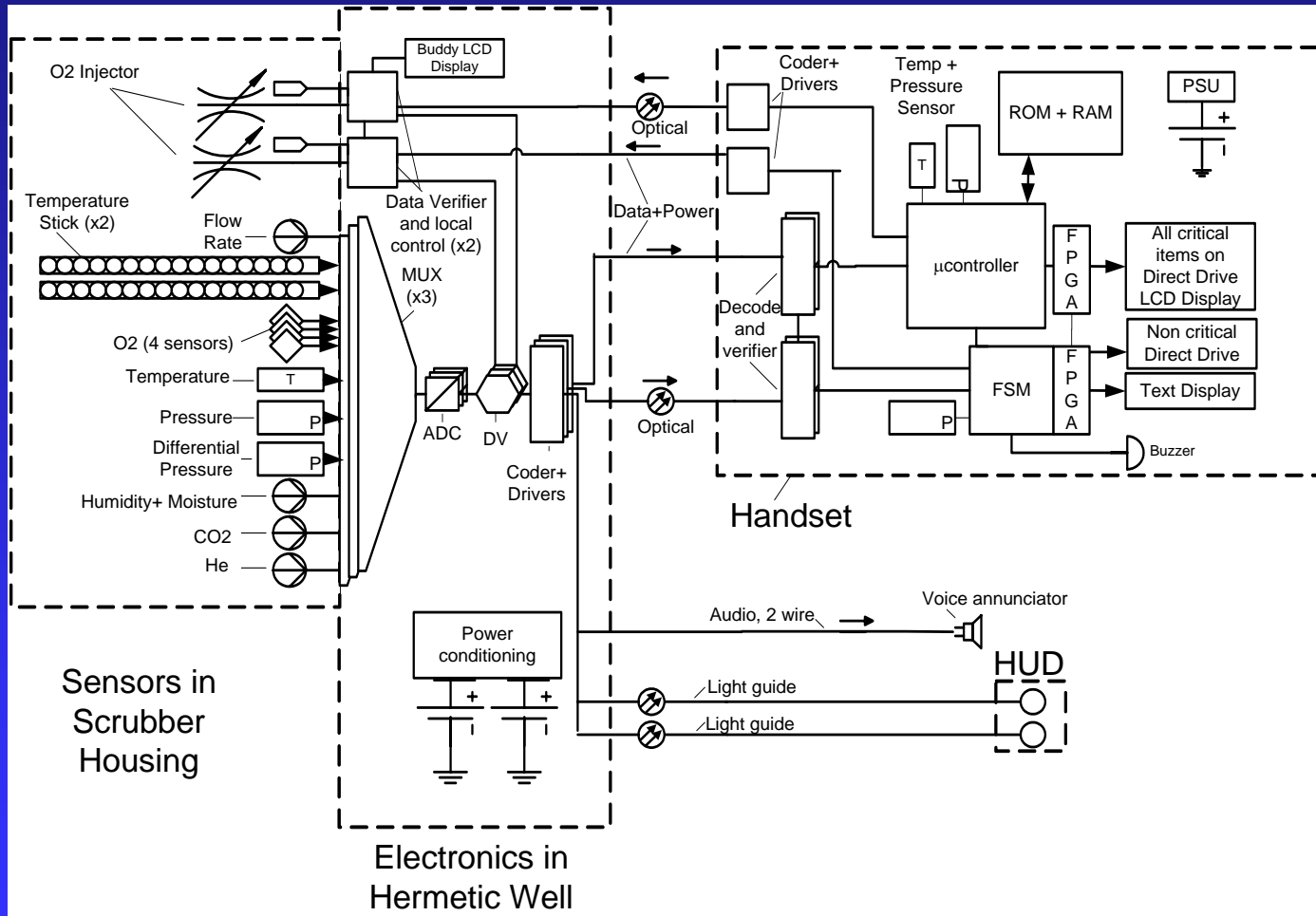
Building On a Solid Foundation

- Runs on a Microcontroller operating in parallel with a Finite State Machine
- That is, two different implementations using different technology
- If one does not produce the same result as other, both ensure a safe state, then self-test, and if it passes, try again
- All is duplicated, 2 uControllers + 2 FSMs, to withstand 2 worst case faults
- Absolutely No Hanging:
 - ✓ **Three independent clock sources, to tolerate failure of clock components**
 - ✓ **Three Independent Power supplies, rechargeable Lithium Ion**
 - ✓ **Three Watchdog Circuits**
 - ✓ **Three Brown Out Circuits**
 - ✓ **Unused microcontroller locations filled with controlled reset vectors**
 - ✓ **State Machine is very sparse, with all spare vectors filled with recovery code**
 - ✓ **All Code verified automatically and independently**

Fault Tolerant Architecture

- Everything is shadowed, using a different technology
- For example, communications between handset and base is
 - Optical using LEDs and polymer fibre.
 - And, Electrical (Using Data over Power Digital Technology)
- This means electrical interference does not affect data
- This also means sharp bends in the cable does not lose data
- All data is sent in packets, with a long checksum, so faulty data is detected (a basic principle in every block)
- Yet, even if the handset cable is severed, CCR continues working at the last set set-point, signalling to the HUD and voice annunciator what the levels are: injectors themselves are intelligent take over in case of failure.
- Every block has a similar architecture, namely a shadow and a means to check if the block and the shadow is working, with means to handle safely the loss of both the block and its shadow.

Fault Tolerant Architecture



Safe PPO2 Control

- O2 sensors have a high chance of >1 failing during a dive, so the O2 sensors are used only for checking not PPO2 control
- Uses automated pre-dive checks to calibrate O2 injector
- Calibration means finding how much O2 the injector injects per second.
- System sends command to injector as a function of the loop delay, and uses the O2 sensors to check result.
- When result not what expected, it can check what the O2 sensors are doing, or if the injector has failed.
- It has an auto-bail out, in case system concludes both injectors have failed.
- PPO2 control is as close to theoretical optimum as tolerances allow, to give PPO2 control to to +/-0.001
- Separate presentation on this feature. Download from:
<http://www.deeplife.co.uk/technologies.php>

CO2 Monitoring

- CO2 monitor uses dual beam Infra Red absorption, with correction factors for pressure, temperature and noble gases
- Rapid response (30 seconds 10% to 90% step, small steps are faster), and accurate to 3% FSD.
- Condensation plate, Hydrophobic membrane and location on warm scrubber stick, avoid failure through condensation
- For backup, CO2 reading obtained from scrubber parameters, but response is slower (several minutes) and less accurate



Full Gas Monitoring

- A by-product of CO₂ monitoring (it is necessary to measure the amount of He, to get an accurate CO₂ measurement)
- Measures He concentration
- Deducting O₂, CO₂, He gives N₂, and END
- Low cost solution, with low power
- Uses just two platinum NTC resistors



Effective Scrubber Monitoring

■ Scrubber Life

- Models scrubber like a battery: it has a life for absorbing CO₂
- Systems monitors O₂ consumed
- Monitors flushes
- From that, calculates how much life is left
- Monitors life by measuring pressure, temperature and flow

■ Scrubber Health

- Temperatures at 18 points are measured
- Flow rate: pressure drop across scrubber is measured
- Capacity remaining from CO₂ consumed
- Gas mix: He, N₂, O₂
- Pressure
- Inlet temperature

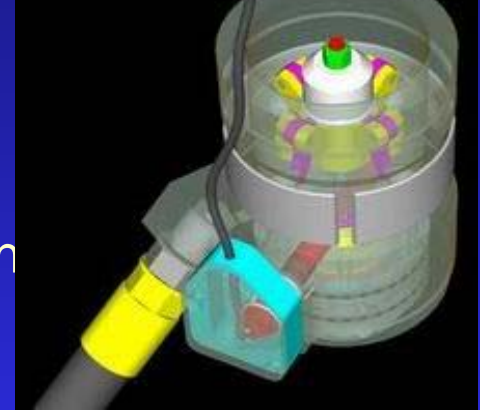
Full Respiratory Monitoring

- Scrubber Health Monitor uses differential pressure sensor
- Without any extra hardware, Respirator Monitor measures respiratory rate and tidal volume
- If respiratory parameters are causing build up of CO₂ in diver, then diver advised to “Breathe Slowly and Deep”
- Escalating to “Risk to death. Shallow breathing. Breathe deep.”
- Scrubber is fitted with a fan, normally used to dry breathing bags after dive.
- Fan comes on when diver is at risk to reduce Work of Breathing to nil
- Same fan dries breathing bags when batteries are being recharged on surface

Auto Shut-off, Dil, Bail-out and Flush

- Named an Auto-ShuDBoF Valve
- Shut off upstream of ADV if breathing mix cannot sustain life
- Adjustable Exhaust on mouthpiece
- Performs auto-flush, when mouthpiece wound down or diver puts his hand over the exhaust
- When breathable again, valve opens
- Fail safe: stays in existing state
- Shutoff has user override cord
- Uses unique balanced design to withstand a fire hose without free flow

3D CAD, showing balanced valve



And in real life



Voice Annunciation

- Voice annunciation is standard on most other life critical systems: aircraft, nuclear, medical interlocks
- Costs peanuts (\$8, a big bag of peanuts).
- Gives verbal warning of fault and recommended action
- Reassures diver, even if they know the action
- Gives advice to those who have forgotten their training
- Gives injector sound when injector operates, so user is aware
- Gives music of choice when all is OK, then voice, then fugues when it is not and action is ignored before repeating voice

O2 Calibration

- Do not let users cal the O2 sensors:
 - O2 cal using “100%” O2 leads to gross errors.
 - For example, if user closes unit and injects O2 until valve pops, then %O2 is usually around 60%, because of large minimum volume (scrubber, hoses etc).
 - If user tells eCCR it is 100%, then DCS risk is high
- Open Revolution solution is:
 - O2 sensors are calibrated whenever scrubber is opened.
 - If sensor at start of pre-dive checks have drifted too far, then asks user to open scrubber so it can cal in air.
 - System does not ask user for pressure: it has multiple pressure sensors
 - Injector system can tolerate ceiling faults
 - Uses pre-dive checks to check max PPO2 that can be achieved on surface, to check sensors over multiple points

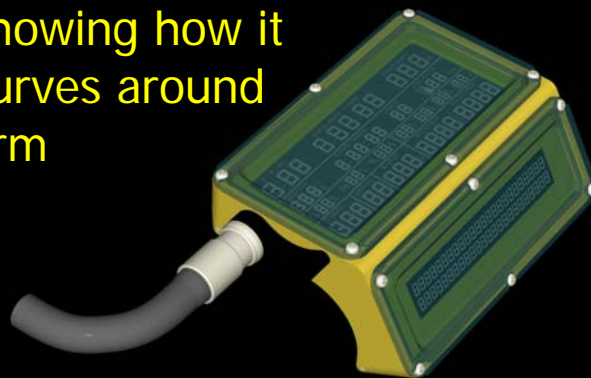
Pre-dive Checks and Self Test

- Every time system starts, it does a 100% self test using JTAG technology, and checks all sensors
- System runs pre-dive checks, with minimal user help
- Cannot be dived if checks do not pass (unless user wants to hold auto-shutoff valve open manually)

Unambiguous Displays

- Main display on handset demonstrator is a dive computer, with full gas analysis, tank pressures etc
- Secondary display is very simple: two lines of text
- First line says what the problem is, or status
- Second line says what to do about it.
- User could dive with no training at all, just look at the text display, and live: not recommended, but this is the standard.

3D CAD Model showing how it curves around arm



Reality



Save the Loony

- System software and firmware is enabled by codes
- Codes determine max depth and what gas mixes are allowed
- Instructors give out codes, issued by factory, and can put time limits on that code. Instructors also have a lockout code which they can use as often as they like
- Beyond allowed depth, or mix, unit warns user
- If warning is ignored, then tells user it will shut off the gas
- If warning is ignored, it keeps shutting auto-shutoff valve momentarily making it very uncomfortable to breathe
- Without pre-dive checks, user cannot dive unless they manage to get to below 10m. When they are doing this, the unit tries to inflate the breathing bag to max
- Has a special “You are a loony. Abort dive Now” message, with voice, fugue and irritating effects.

Summary of Solutions

Deep Life Technology	Benefit
Safe O2 Injection	Maintains PPO2 within safe limits, tolerating all O2 sensors failing in any mode
Effective Scrubber Monitoring	Scrubber Life Monitor and Health Indicator detects accurately whether the scrubber is working and the portion of scrubber life used.
PPCO2 Monitor	Accurate PPCO2 monitor, operating at any depth and with any gas mixture.
Full Gas Monitor	Shows complete analysis of breathing gas, in real time.
Combined Auto shut-off, auto bail-out, auto flush and auto diluent valve.	Ensures the user is always breathing a safe gas mixture.
Voice annunciation of alarm states	Uses a piezo in the mouthpiece to provide verbal indication of fault and recommended action. Supplements HUD and Handset displays.
Full Respiratory Monitoring	Prevents faults that cause an increase in the Work of Breathing from affecting safety.
Fault tolerant CCR architecture	Allows a CCR to withstand two worst case faults, and scores of random faults. This compares with contemporary CCRs which cannot withstand any worst case fault and only one random fault.
Total Compliance	With Open Revolution 1 billion hour requirement, meeting EN14143, HSE proposals and OSHA requirements for rebreather safety.