DEEP LIFE OPEN REVOLUTION FAMILY OF REBREATHERS

Failure Mode, Effect and Criticality Analysis Volume 3:

Electronics Failure Mode Review

DOCUMENT: [Filename]	FMECA_OR_V3_Elec_FMA_090529
ORIGINATOR:	**Dr. Alex Deas, Marat Yevtukhov, Alexei Bogatchov, Dr. Bob Davidov, Dr. Vladimir Komarov, Dr. Sergei Malyutin, Dr Oleg Zagreblenny, Dr Sergei Pyko, Igor Abrosimov, David Coyne**
DEPARTMENT:	**Engineering**
DATE UPDATED:	**29th May 2009**
REVISION:	**G**

APPROVALS	
__/AD/_____ Project Manager	___29th May 2009_____ Date
__/VK/_____ Quality Officer	__29th May 2009_____ Date

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

Revision History

Revision	Date	Description
A	18 May 2005	Update to DL RB
B	10 July 2005	Review of preliminary circuit diagrams, based on circuits used in Prototype III.
C	18th Nov 2005	Completion of Review to Prelim Submission B level. B1 with volume numbering update only.
D	16th Feb 2007	Update to include circuit changes resulting from test programme over the past year 18th Dec 2006, and on 16th Feb, accepted changes to remedy ALARP issues identified during EN61508 compliance reviews.
E	4th Apr 2007	Full review of Rev C
F	2nd Feb 2008	Capture of the validation findings on Rev C, and the consequent ECOs
G	29th May 2009	Updated for EN 61508 compliance purposes.

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

Table of Contents

1 PURPOSE AND SCOPE

This is a Failure Mode and Criticality Effect Analysis (FMECA) of the electronics in the Open Revolution rebreather controllers. It forms Volume 3 of a set of 8 volumes of FMECAs covering the Open Revolution rebreather system.

This data for this FMECA comes from four sources:

1. A section by section analysis of each version of the rebreather controller electronics, by a team of highly experienced electronic design engineers.
2. The capture of all problems identified during circuit validation or verification tests that involve the electronics.
3. Modelling and simulation work on the Open Revolution rebreather.
4. Review of the failure mode in the event of each component failure, forms Volume 2 of this FMECA. Only the overall circuit diagrams are reviewed in this volume.

Extensive reference is made to Volume 2, for the MTBF of each of the circuit blocks and subsystems. Deficiencies in MTBF data are noted in respect of certain components, that are then addressed by circuit changes discussed here.

The scope of this document is all failures that originate in the rebreather electronics.

The rebreather circuit diagrams accompany this document. For completeness, these are in the form of Submissions A, B, C and D.

- Submission A is the original prototype used to demonstrate particular technologies: it was not intended to be dived outside a closely controlled test environment. Two samples of Submission A were fabricated and tested.
- Submission B is the first attempt to produce a safe circuit design. It failed internal EN61508 reviews, as described here. Five samples of Submission B were fabricated and tested, purely to test the underlying technologies.
- Submission C was designed to correct short comings in Submission B and to meet all EN61508 requirements in full. Extensive trials were carried out on this circuit, including thousands of chamber runs and over a hundred manned dives. It failed some of these important verification tests, and also failed a motivated independent review that considered every net for noise, failure conditions and suitability. Sixteen samples of Submission C were fabricated and tested.
- Submission D addresses all issues in Submission C: it is a series of Engineering Change Orders to remedy each fault found during verification tests: each of these, were tested by reworking the Submission C samples, before incorporating them into the pcb layout for production.

Review of all Submissions are included here, to avoid any possibility of any of these faults recurring in the future, and also to propagate a wider understanding in the industry of safety critical system design.

This review covers the base unit, sensor board, scrubber stick and handset. The PFD is included only in the base form (that is, with LEDs and voice annunciation). It does not include the PFD. Neither does it cover the independent CO2 monitor, O2 monitor or dive computer: the review of those circuits forms FMECA Volume 9 of this set. The handset that formed part of Submission A is included: this was removed at the Submission B development point in favour of an intelligent PFD to tighten the interaction between diver and the key PFD monitor.

This document is a working document, that is added to at each of the Stage Reviews and will not be finalised until all component changes are finalised in the pre-production prototype.

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

Reference is made to the Project Green Book Specification and prototypes.

The rebreather controller (Base Unit) has been formally assessed as SIL 3+.

2 CIRCUIT REVIEW OF SUBMISSION A

2.1 Sensor Board

The circuit diagram is attached, in Annex A.

The function of the sensor board is to:

1. Provide readings of O2, with quad redundancy
2. Provide a pressure reading, used to measure depth and used in conjunction with the Scrubber Stick to determine scrubber health.

Provide a humidity sensor.

Only Functions 1 and 2 above are critical functions. Redundancy of Function 2 is managed by the Scrubber Stick review.

2.1.1 Sensor Board Page 1

No issues.

2.1.2 Sensor Board Page 2

Two issues were raised: risk of bitmetallic errors and corrosion, and the error introduced by the op-amps on the board.

The pressure sensor and humidity sensor on the sensor card is accepted. The humidity sensor is an optional element in the design.

Debate on whether the temperature sensor is needed. It is a provision in the design that is not normally fitted. There is no useful correlation between the temperature of the gas leaving the scrubber and the scrubber efficacy or scrubber life: none of Deep Life´s scrubber monitoring techniques use such a sensor. There is an ambient temperature sensor in the handset and the scrubber stick collects the temperature at 16 points in the scrubber. Given this, there seems to be no use whatsoever of measuring the scrubber exhaust gas.

Decision: remove the temperature sensor on the sensor board.

2.1.2.1 Bitmetallic Error and Corrosion

An error can be introduced from the bimetallic effect of the contacts from the O2 sensor to the base board. There are 2 contacts to consider.

a. The connector on the O2 sensor itself. This is tin on copper, or gold on nickel on copper.

b. The connector from the sensor board to the base board.

If these contacts are copper to gold, then for every contact, there is a complement. This means that the bimetallic voltages should cancel.

If the contact is tin, then the tin forms a eutectic producing a bimetallic voltage under under a microvolt.

Bitmetallic corrosion risks in sea water are minimized with a tin finish because tin is next to brass in the galvanic series. For a gold finish, significant risk exists, with reference to http://www.npl.co.uk/ncs/docs/bimetallic.pdf

Decision: All contacts should be tin on brass and not gold on copper or brass.

2.1.2.2 Error from Op-Amp Drift

The review team would like to see no active components at all in the breathing loop, due to risk of a die short or other fault that could cause noxious fumes.

On the Op-amps used to buffer the O2 sensors, these are extremely low drift opamps from Analog Devices that the team have experience of: their noise, stability and drift performance exceeds that of chopper stabilised amplifiers. However, the drift over a 30 degree temperature range is 2.5uV. Given a worst case O2 signal of 7mV, this amounts to error in the 11th bit of resolution. This error is greater than the 2 bits of resolution that can be lost in the ADC if no opamps are used. That is, the ADC is 24 bits and completely linear, with 1.25V FSD. The maximum signal from the O2 sensor is 206mV (PPO2 showing 3.2 before any limiting is permitted to occur, and new sensors with 13.5mV output in air). Therefore, the design is more accurate with the buffers removed.

Decision: remove the buffers and route the O2 signals as a differential signal directly to the ADCs.

2.1.3 Sensor Board Page 3

This page consists of Solenoid or Stepper Motor drivers. The injector valve is either a solenoid injector valve with two solenoids on one valve, or the Deep Life injectors which are either a variable orifice valve or a silicone pinch valve both of which are driven by either a DC motor or a stepper motor. The drivers handle all of these variants, as well as handle the linear Hall sensors that detect the position of the valve.

The question is why are these circuits on the sensor board instead of the base card. The linear Hall effect sensors measure a 1mm displacement on FSD, so produce a low level signal.

After debate, the review team were unhappy about having any active components such as these in the breathing loop and it was decided to move them back to the base card.

Decision: Move all circuitry on Page 3 of the Sensor Card to the Base Card. Decision affects Page 4 also.

2.1.4 Sensor Board Page 4

Same decision as for Page 3.

2.1.5 Sensor Board Page 5

No issues except that all connectors should be tin on brass, not gold on brass, with the connection being gas tight.

The connectors should be DIN 41612 birfuricated contacts, not Molex single wiping contacts. The bifuricated contact should be one which cuts into the tin to form a joint. This is then relatively immune to moisture ingress. The life of the contact is low, but the number of times the sensor board is mated with the base card should be just once, and needs to be tracked during manufacture.

2.2 Scrubber Stick

The circuit diagram is attached, in Annex A.

The function of the scrubber stick is to:

- Provide temperature readings at 16 locations through the scrubber. This allows for 8 temperature sensor readings in the case of half the temperature sensors failing, and more accurate scrubber monitoring when all are functional.
- Provide a CO2 reading
- Provide a temperature compensation reading for the gas in the CO2 sensor path
- Provide a He reading
- Provide a pressure reading for the gas prior to the scrubber, which in conjunction with the pressure sensor on the Sensor Board, provides a reading of the differential pressure across the scrubber for scrubber life and health monitoring purposes.

All these functions are critical, other than the He sensor and temperature of the CO2 path, failure of which simply increases the error band, but given the logarithmic nature of CO2 build-up, this does not have a significant impact on health.

2.2.1 Scrubber Stick Page 1

No issues.

2.2.2 Scrubber Stick Page 2

This comprises 16 temperature sensors (NTC resistors, 1206 size to ensure sufficient contact area with the wall of the stick), and a 50uA current source.

The NTC chain varies in resistance from hundreds of ohms to tens of K ohms. This means the chain cannot be supplied by a fixed resistor driven from a voltage reference for the current source.

There are no tantalum or electrolytic capacitors: all capacitors on the current source are ceramic so do not pose a fume hazard.

The MAX407 opamps are chosen because of their very low power consumption. Both are in one package, but as the package is part of one circuit this does not create any more failure points.

If the current source fails, the temperature readings can be max or zero. Both error conditions would signal a scrubber failure, so the circuit is fail safe.

The review team then considered the fault tolerance of the circuit and determined that there is a risk of the current source providing a current which is neither max or zero, but simply adrift. This means the circuit submitted for review is not 100% fail safe. There was no provision to monitor the current. If one NTC were to be a fixed resistor, then the current can be monitored, and if incorrect, the digital logic can correct for it. In this case the circuit is both fault tolerant and fail safe.

The NTCs were found to be fragile in service. Replacement with I2C digital temperature sensors was considered, but the I2C chain causes either a large increase in the number of

tracks to be routed with its attendant reliability issues, or in daisy chain, reduces the MTBF and MTBCF by a factor of 12 to 15, depending on how many sensors are fitted. The most robust solution is to use National Semi LM35 to LM61 series sensors.

Decision: Change the design to use Nat Semi LM35 and LM61 temperature sensors with a voltage output, instead of the NTCs. The 15 temperature measurement points are overkill, based on a review of the data measured by temperature sensors in active scrubbers: they can be reduced to 12 sensors.

Due to a further design change in Rev C, the MAX407 are replaced by Analog Devices low noise chopper type amplifier.

2.2.3 Scrubber Stick Page 3

Pressure sensor and temperature sensor, circuitry has no issues.

The resolution of the pressure sensor is considered. The sensor is 15 bits resolution, at FSD. This means the least significant digit represents 427 microbar. The pressure drop across the scrubber is typically 12 to 14 mbar (measurements on the Draeger scrubber filled with Sofnolime), and the ExtendAir cartridge is 10mbar. This means that there are 20 values representing the respiration cycle: sufficient for WOB monitoring, and for scrubber life monitoring.

When the temperature sensor fails, the CO2 reading can be in error by up to 20%. This is not a critical failure.

When the pressure sensor fails, it would not be possible to monitor WOB and also the scrubber health monitor would show substantial error. This means that if any of the three pressure sensors fail, the dive should abort.

The MTBF of the pressure sensor was missing and the manufacturer is being contacted.

The MTBF of the connector and pcb is better than one in a million hours.

2.2.4 Scrubber Stick Page 4

This contains the electronic for the CO2 sensor: the IR source and detector.

The top portion of the circuit diagram drives the IR source. This is a bulb with 40,000 hours MTBF. Failure of the bulb gives a zero output from the detector and this fault condition is flagged by the digital electronics.

2.2.4.1 IR Source

There is an op-amp on the voltage reference to generate a 4.5V reference, to power the bulb. This opamp is a MAX407 micropower opamp. The MAX325 is a chopper, which switches between ground and the voltage reference. The output from the chopper drives the bulb via a MAX407 and a transistor.

Decision: Move the decoupling tant to the Base Card, as it represents a fume hazard.

2.2.4.2 CO2 Sensor Receive Path

Decision: Replace the 10uF and 47uF capacitors with ceramics to eliminate the fume hazards, with resistor changes to keep the time constants on the opamp feedback loop the same.

Decision: Move the MAX660C and the 220uF to the Base Card so it is out of the breathing loop. Both the chip and the capacitor represent a fume hazard otherwise. There is already

circuitry on the Base Card that can be reused to provide this reference, so this move could cut down the BOM.

2.2.5 Scrubber Stick Page 5

This contains the Helium sensor.

Failure of the helium sensor causes an error in the CO2 reading by 50%. This is not a critical error given the logarithmic nature of the CO2 levels.

Failure of the helium sensor is needed also for decompression calculations. This is a critical value. This requires the sensor to be checked and monitored. Any of the failure modes of any component, cause the output pulse to stop. This can then be detected and the diver asked to use manual tables.

If the sensor itself drifts, or the current source changes, then the He sensor will in error. So there should be a resistor to allow an ADC on the Base Card to verify those items.

Decision: Add a current source and flow monitoring resistor to provide fail safety.

Decision: Move the tant C24 to the Base Card and use a ceramic capacitor locally. This eliminate a fume hazard.

Decision: Cover the components with silicone gel, in addition to the conformance coating normally applied, to produce an extra measure of protection from water damage to the devices.

2.3 Base Unit

The architecture of switching the batteries instead of running parallel batteries and power supplies then simply connecting the outputs of the regulators in parallel was reviewed. The arrangement in the circuit diagrams allows each battery to be monitored, and if any battery drops or has a brownout, then to switch in another battery immediately. This way the circuit runs of one battery at a time, but there is a redundant switching in of the spare batteries when there is a problem. The advantages of this route are:

1. One always knows from which battery the system is operating. The battery is monitored both by the two ADCs (FPGA and uController), as well as by specialized voltage monitors (e.g. U4). The ADC outputs are used to predict battery life and status.
2. Each battery is monitored by its own voltage monitor and brown out circuit. For example U4 for the main battery and when the battery drops, U4 changes state to 0. The FPGA and the uController each see the output from U4, then the controllers each switch the batteries. This switching is within a few microseconds, so the regulator circuits do not suffer any glitches.
3. The regulators are individually redundant rather than being tied into a block containing a battery. This improves the overall MTBF of the circuit.
4. The cost of the switching FETs is less than use of redundant power regulators.

On review, the power supply architecture was passed.

2.3.1 Base Unit Page 1

No issues.

2.3.2 Base Unit Page 2: Main Battery PSU

The circuitry on this page shows the provision of the battery supply to the regulators. There are three batteries to source power, only one of which is used at a time. The batteries are the MAIN (on J4, J5), AUX (on J6, J7) and **from** the Handset battery (on J8, J9 on Page 3) and redundant power is sourced **to** the handset (on J2 and J3). The batteries are Lithium Ion Gel Polymer cells, soldered onto the pads on the board, and fixed rigidly to the boards. The fixing has had extensive testing: it stands up to being dropped 10m onto concrete without the battery contacts pulling away from the board.

The circuitry comprising M2, M10 and M9 is to switch the charger onto the main battery. It is cheaper to have this group of FETs than duplicate the charger. The charger is on page 3 of the schematics (top left),

U4 is a Brown Out Circuit and voltage monitor. This is set to trigger at 2.6V for 100uS. The reason this circuit is present is to measure the battery voltage and signal to the FPGA and uC within 100uS of the battey falling below 2.6V. This gives sufficient time for the FPGA or uC to switch in an alternative battery.

The FPGA and uC knows the actual voltage available from each battery from the ADC reading. The priority to batteries is MAIN, then AUX then HANDSET.

L1, L2 and C11, C12 is to filter the data from the power on the HANDSET: the connection to the handset uses data over power technology for noise immunity and to reduce the number of connectors and the size of the cable. The circuit on Page 2 to the Base Unit Pads, provides power TO the handset. Power FROM the handset is on Page 3.

U2 is the data over power, differential transmitter to send and receive data up the cable to the handset over the power line. The same circuit is used at the other end of the cable, in the handset. U2 is redundant with the optical fibre, which is used to send the same information across the optical medium. The outputs from U2 and from the optical signal, is checked for checksums in the FPGA and uController. The U2 data is used only if the optical signal has a corrupted checksum, or is absent.

2.3.3 Base Unit Page 3: Battery Charging Circuit

The charger supply charges the batteries, being switched to charge one battery at a time. The sequence is MAIN, AUX, then HANDSET. This sequence is used for safety, as the unit will operate without a handset, but the user is unlikely to use the unit if they see the HANDSET has a low battery.

The external supply is used to power all the circuitry in the base unit when the charger is connected. This means the FPGA and the uC can monitor the charging process and avoid things that could damage the batteries. For example, even though there are three batteries to be charged, the batteries are not discharged before charging again as Li Ion has no material memory effect. The FPGA and uC also protect the batteries from excessive charge currents, monitor the charge cycle. The max charge current is set by R14.

The charger circuit uses a special Li Ion charger IC, U1, which works by first providing a constant current then a constant voltage. The charge fault and charge status lines are monitored, to provide feedback on battery health. Defective batteries are reported to the user during charge and the unit will not permit diving with a faulty battery without specific manual override.

Decision: Check the manual override provision in the software and firmware.

Power from the handset is received on J8 and J9 on Page 3 with its dedicated voltage monitors and switching circuits, in the same design as used for the MAIN and AUX batteries.

Base Unit Page 4: Power Supplies

This provides dual 5.5V supplies using a switching regulator (dual for redundancy, as the switching regulator is less stable and has more components that linear regulators). This is followed by a chain of linear regulators for 5V, 3.3V, 2.5V and 1.2V.

Decision: MTFB data indicates the risk of failure of this chain is outside the design targets. The design must be changed to comply. The concern was that failure of any of the linear chain, would mean failure of the base unit. If the failure was very abrupt, there would insufficient time to cut off the shut off valve, so failure of this chain would be a critical failure. Two separate 3.3V power supplies cannot be used because this voltage is used for the scrubber stick's senors and the pressure sensors on the sensors card, so parallel the 3.3V and 5V regulators to provide redundancy.

Decision: The microcontroller needs only 3.3V, so to improve the MTBF to the target levels, two 3.3V regulators should be arranged in parallel (i.e. with dual redundancy). The 3.3V regulator should come off the 5.5V supply directly to the uC.

Decision: the 2.5V supply 2.5V power supply should be always on otherwise FPGA will lose its configuration, and should come from the 5.5V supply.

Decision: The drop from 5.5V to 5V in the first linear regulator is not sufficient energy saving to make it worth putting in a chain to the 1.2V supply which is the main supply for the FPGA, so the 1.2V supply should also come off the 5.5V supply.

The 5.5V switching regulators is designed to step up the 2.6V to 3.2V, and is dual redundant. These tolerate the 7.2V which can be produced from the Nokia charger if the batteries are all open circuit.

Decision: The 1.2V regulator does not need to be chained with the 5.5V switching regulators. Take the input to them from the combined batteries line. This can also tolerate 7.2V from the Nokia charger should the regulator on that line fail: the maximum input voltage is 15V.

The 5V regulator can withstand 20V on its input and has just 20mV of dropout so the configuration of 5.5V switching regulator

2.3.4 Base Unit Page 5: Primary ADC

This uses a 16 input Sigma Delta 24 bit ADC to measure all sensor values, with the scrubber stick thermistors MUXed on the stick. The ADC is well known to the Design Team, and reviewers, with excellent characteristics: simple, avoids software errors, minimal external components, inexpensive, perfect linearity and extremely good accuracy.

U21 are the buffer amplifiers for the ADC. It is noted that the supply is 3.3V.

Decision: There are now two 3.3V supplies. The supply names should be changed, with the FPGA and the Primary ADC having one supply, and the uC with the secondary ADC with the other supply. Both FPGA and uC can read both ADCs.

Decision: U23 is powered from 5V. It provides greater redundancy to power it from 3.3V: it is a MUX to provide the battery voltages and power supply voltages to the ADC for monitoring purposes.

U13 is a the voltage reference serving both ADCs. It is therefore a single point failure risk. The reference is not cheap, at $7.57, plus ancillary components. The output is buffered in triplicate redundancy, but the reference itself is singular. If the reference fails, then all sensors fail. The reference is about the same price as the ADC.

The three reference buffers are chopper stabilised amplifier equivalent, with zero drift. One buffer is for the Primary ADC, one for the Secondary ADC, and one goes to the Scrubber Stick for the CO2 sensor and the He sensor. These chopper stabilised amplifiers are used everywhere there is a need for zero or low drift: most of the signals are DC or near DC.

Having a single reference makes a nonsense of power supply redundancy, because if the supply to the reference fails, then it takes out both ADCs.

The options are to have a fall back circuit so when the reference fails, the ADCs work but with reduced accuracy (only 8 bits accuracy is needed, except for the CO2 sensor which requires 12 to 14 bits).

Decision: Put in a cheap reference for the Secondary ADC, as both FPGA and uC can read the Primary ADC when it is working. Apart from drift, we can calibrate the reference for the Secondary ADC, using the Primary. The cheapest reference is just a resistor divider from the power supply. Next up is a zener diode. Spend the 2mA on the Zener diode, with calibration at every watchdog interval, checking the Primary ADC is correct and within range, then calibrating the secondary. Then when the Primary fails, the readings from the secondary should be very close, so there is not a discontinuity in readings. After that point, where the Primary has failed, the readings will drift apart but not by an amount that endangers the user.

Decision: There is just one Analogue Ground. There should be one per ADC. This means that everything on Page 5 has one Analogue Ground, and everything related to the Secondary ADC has a different ground point, with the two ground points connected by single wire (represented as a 0 ohm resistor so the EDA tools treat them separately. The grounds are star connections. Digital grounds are planes. Digital grounds do not cross analogue grounds. This grounding arrangement was debated and approved by DL´s signal integrity team, and proven on the high performance PMU.

Base Unit Page 6: Secondary ADC

The same circuit configuration as on Page 5, so the same comments and decisions apply.

Decision: The voltage reference for the Secondary ADC should be moved to Page 6 (from Page 5).

Base Unit Page 7: JTAG Board Test and FPGA Configuration EPROM

U26 is the configuration EPROM. U31 is part of the main FPGA that handles the configuration. There is a JTAG port on the board for automated testing, and for the programming of the EPROM. The EPROM can be configured either through the JTAG interface, or partially configured via the USB interface within the FPGA: this is to enable the user to load firmware upgrades via a PC. The JTAG interface is J13, and is accessed directly on the base board: this is the same for the handset.

There is separate provision for the failure mode where the EPROM is corrupted or the FPGA fails to load (on Page 9).

Decision: Remove U55 and put into the JTAG cable, as the user does not need them or the associated circuitry.

Base Unit Page 8: Clock Generators and USB Transceiver

USB is implemented within the FPGA, but a transceiver is used to provide the correct voltage levels and protection. The USB circuit is a proven one, and is not a critical function.

The clock uses dual redundancy, as a single clock has an MTBF of only 100k to 1mn hours. Failure of the clock is a critical failure: the microcontroller would hang, and the FPGA would not progress from state to state. To achieve more than 10 billion hour MTBF for this circuit block, two clocks are provided.

Decision: The clock still relies on U42. This does not meet the MTBF target. To resolve this U42 should be rearranged across two devices, one driving the FPGA and primary ADC, the second driving the uC, secondary ADC. This then achieves the 10 billion hour MTBF requirement for this circuit block. The clock for the boost converter and the pressure sensor. There are two pressure sensors, which should be driven by different clocks. As

both clocks are crystal sources, the frequency error between them should be less than 100ppm.

Base Unit Pages 9, 10, 11 and 14: FPGA and uC with Provision for FPGA or uC failure

The problem addressed by this circuitry is that if the uC fails, or the FPGA fails, then the outputs can be in a state that blocks the ADC or the injector. The uControllers in common use in dive systems have an MTBF of only 60k to 100k hours. This is a grave risk, that requires use of parallel FPGA and uC: which is what the design under review uses, to reduce the overall MTBF better than 6 billion hours.

A circuit acting as a set of Exor gates allows the uC to disable the FPGA and FPGA to disable the uC when either fails in a state which blocks the outputs. That is the FPGA monitors the uC and the uC monitors the FPGA, and if either fails, then the working circuit will disable the outputs of the failed circuit, using a circuit arrangement such that a failing circuit cannot block a good circuit (the circuit only has to block the active state, and if the active state is the inverse of the normal failure state, then the whole arrangement is fail safe).

This circuit uses many Exor gates. While Exor gates are cheap, they take up space and create extra failure points.

Decision: After discussion, a simpler circuit as shown in Figure 1 below, should be adopted.

Base Unit Page 12: Secondary Clocks

Decision: The division of Exor Gates to duplicate the final stage, taken for the primary 8MHz clock, should be applied to this page also.

Counters are used to create the secondary clocks from primary clocks.

Base Unit Page 13: Connectors

No issues.

Discussion on use of SMD or through hole connectors. The latter are preferred.

Base Unit Page 15: Fibre Optics

Communication between base and handset is via both electrical and fibreoptic medium, for reasons of redundancy, tolerance to EMC and reliability. The electrical connection uses data over power technology as described earlier. The fibre optic line uses a large 1mm diameter mulitcore polyester fibre with RED LED source so the transmit operation can be checked easily by a user.

Decision: A lot of EXOR gates are used as simple buffers. These were used to use spare gates, but there is now enough to use buffers which are 6 in one package.

Decision: Signals that go to both FPGA and uC should have the buffers doubled up, as otherwise a short on the FPGA will take down the signal for the uC also.

It is noted there will be two new pages, as circuitry reviewed in other portions of the design migrate to the base unit as a consequence of this review.

2.4 Handset

The same comments about the base board apply to the Handset. The review decisions should be implemented in the handset also.

The MP3 player is in the extended PFD and no longer in the handset. The reason for this move was to eliminate unnecessary functionality from this important safety critical unit.

Decision: Review the storage for dive profiles with the software team to ensure it is sufficient for 250 hours. In performing accident reviews, it was found that a sampling interval of 10s used by the VR3 is not sufficient. The dive profile and all parameters should

be stored every 3 seconds if the depth differs by more than 10% from the previous sample, otherwise a 15 second sample time is sufficient.

Decision: Review whether dive profile storage space can be eroded by MP3 files..

DRIVING CONTROL LINES (I.E. PRESSURE SENSORS LINES, POWER SWITCHES LINES, MUXES LINES)

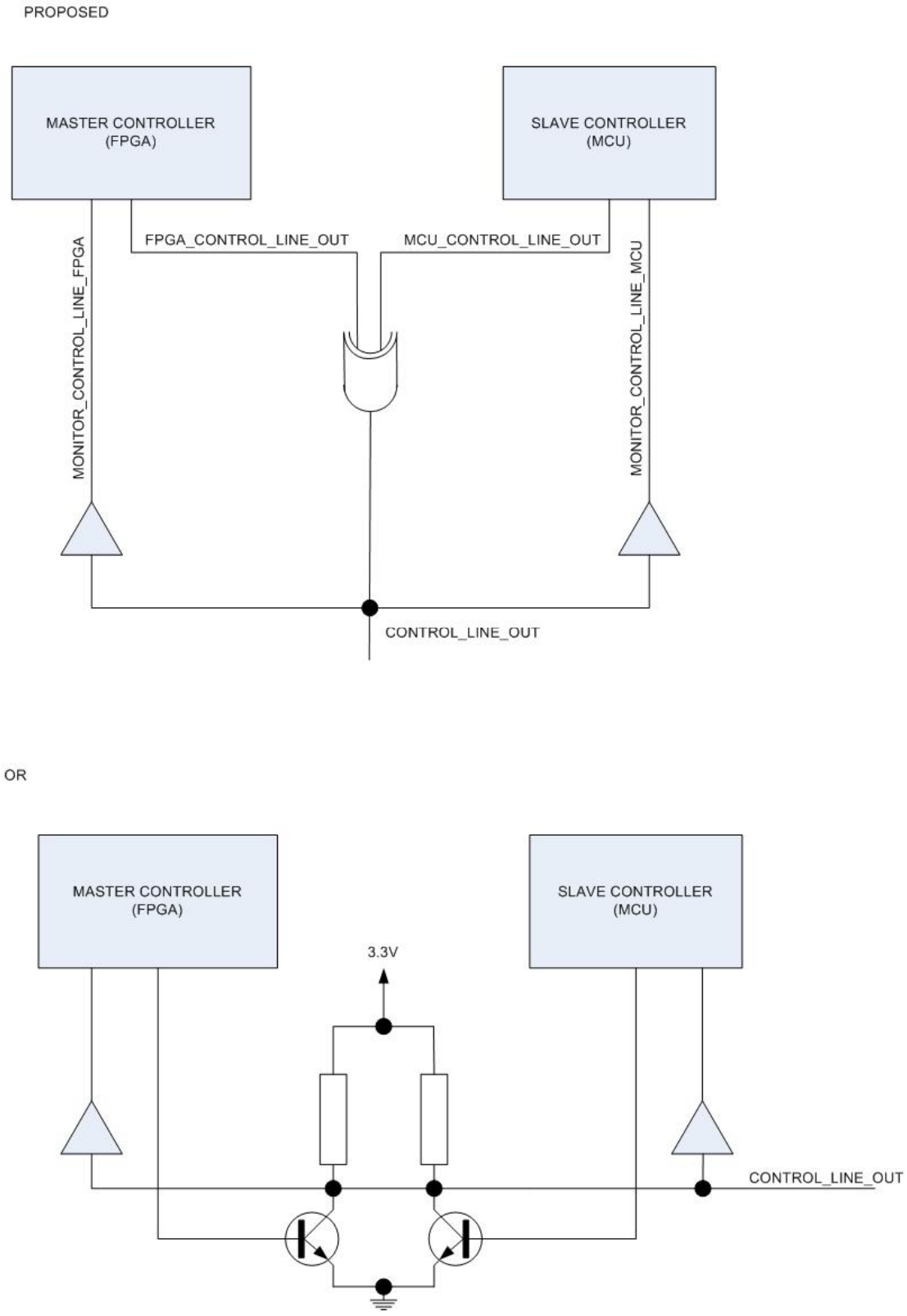

Figure 1: Simplified Circuit to prevent FPGA blocking uC and visa versa

-

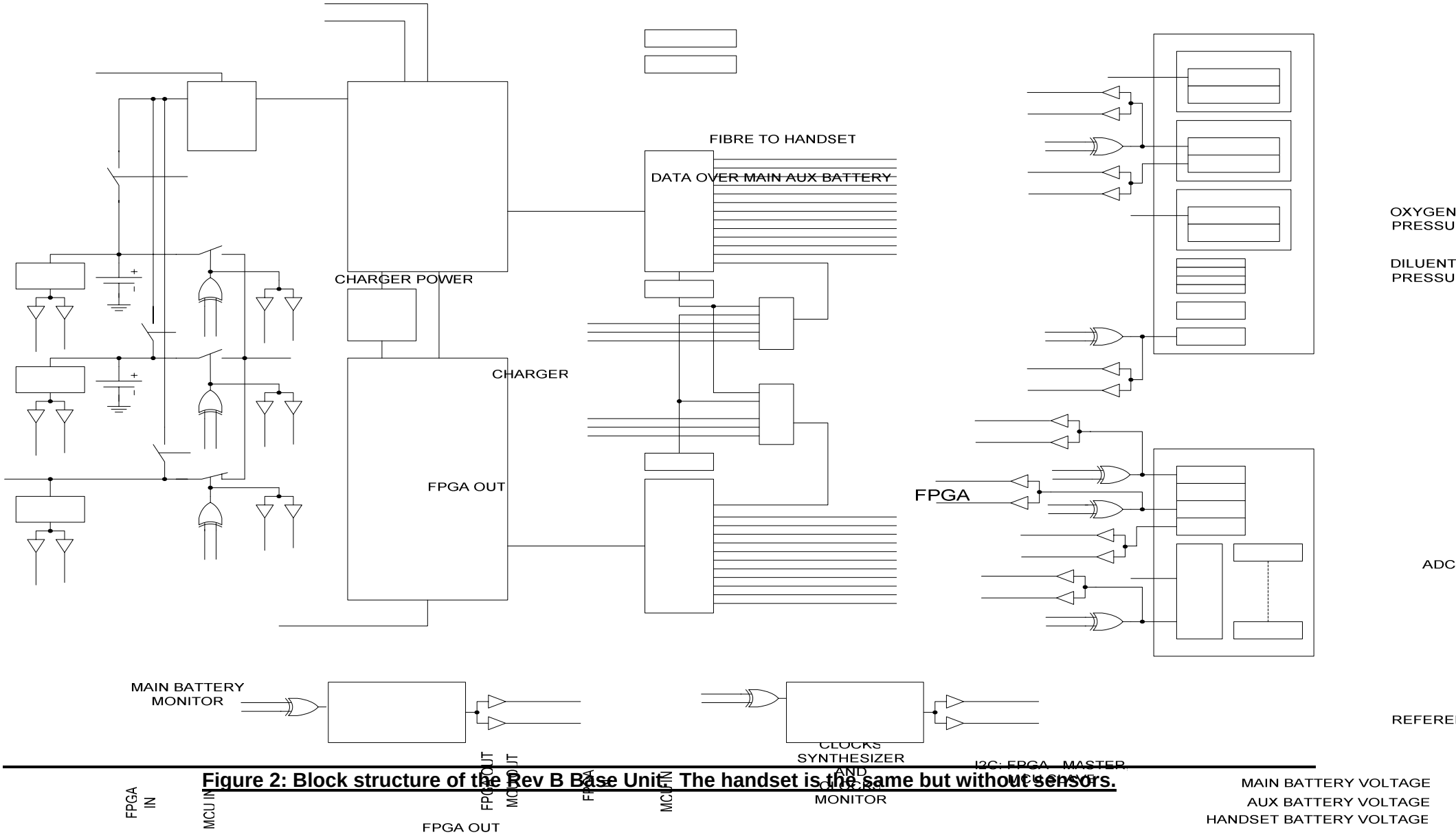

Figure 2: Block structure of the Rev B Base Unit. The handset is the same but without sensors.

3 REVIEW OF CIRCUIT REVISION B

Circuit Submission B was reviewed to check that each of the decisions had been implemented, or adequate rationale provided.

Submission B was passed for board layout.

A further review of the circuit will be made when the board layouts are available, to ensure the circuits are implemented according to the Design for Production guidelines within the quality procedures of Deep Life Ltd, as well as giving time for the reviewers to consider any further points on the circuit.

Submission B failed EN61508 compliance reviews, with the corrective actions implemented as noted in the review of C below.

4 REVIEW OF CIRCUIT REVISION C

Revision C of the electronics incorporates all design changes from earlier safety reviews, from testing, and from EN61508 compliance reviews.

The major changes are:

- Change from Xilinx Spartan FPGA to Actel Pro-ASIC 3 to eliminate the risk of FPGA configuration upload during startup being corrupted, in the transfer from external Flash memory to the FPGA. The FPGA is a highly reliable, multiply redundant design.
- Change from Microchip PIC series microcontroller to ARM 7 based microcontroller, to enable White Box verification of the system: ARM 7 is a formally verified processor, with open compilers and debuggers available, whereas PIC has never been formally verified and the compilers are closed and are unverified. The microcontroller operation is that of a continuous monitor of the FPGA, with a hardware protocol such that when the FPGA fails, then the microcontroller can flag the failure and maintain life critical functions until the dive is aborted. The microcontroller has a lower safety integrity than the FPGA, but is only used when the FPGA fails, and for secondary safety computations, so the microcontroller requires to be only a low availability safety system.
- Routing of oxygen sensors changed to eliminate the risk of an single ESD discharge, or open circuit sensor with a high voltage, from destroying all oxygen sensing ADCs. This has required use to separate ADCs for FPGA and microcontroller.
- Batteries changed from 3.6V cells with step up regulation, to 7.2V Valence safety batteries. Triple redundancy of the batteries, or power source, is maintained.
- Power supplies were completely separated for the FPGA and the microcontroller, so the system can be treated as two quasi-independent controllers.
- Active testing of the oxygen cells to verify type, current ceilings and to detect electrolyte leakage.
- The ESD tolerance for the oxygen cell channels was increased to a 25KV HBM target.
- On-off algorithm improved to reduce current during “off” mode, but with fast switch on when PPO2 falls below trigger levels.

- Merge of all components onto one card, because the flexible connector linking the power supplies to the FPGA and microcontroller board was found to be unreliable, and there was excessive noise from the power supply card to the signal conditioning circuitry.
- Improvement of USB port, changing from USB 1.1 to USB 2.0 for wider compatibility.
- Pressure sensor duplicated inside hermetic volume, that is with silicone oil fill, to prevent sensor damage and offset drift due to helium migrating across material stress lines.
- PCB tracking improved, with all signals moved to inner layers, with only guard ground area on the outside, to enable the system to tolerate extreme magnetic flux densities during underwater welding or cutting operations[1]. The housing material was changed to Kynar which is an electrolyte, to provide a further screen. A mu-metal screen is added over the active components.
- The scrubber stick pressure sensor was changed to a true differential sensor, tolerant of helium.
- A specialized carbon monoxide and hydrocarbon sensor was added to the scrubber stick.
- An additional ADC was added to the scrubber stick to improve tolerance to high levels of environment electrical noise, so only digital signals travel from the scrubber stick to the base unit.

The overall design has been formally assessed as SIL 4.

The circuit diagrams reviewed were:

- Scrubber stick, 21-3-2007 13:28, Rev C
- Infra-red sensor mezzanine card, 21-3-2007 13:28 Rev B
- Sensor card, 23-3-2007 11:23 Rev C
- Base unit card, 28-3-2007 8:28 Rev C

These are considered in turn, after the pcb and component screening.

4.1 PCB Layouts

Each pcb has a set of detailed layout rules.

Every pcb is a multilayer card with all signals routed internally and clean ground plane not used for ground routing on the outside layers. All external planes are connected to the metal plate over the sensor card, which is connected to the sea water via the electrolytic action of the Kynar. This means the ground moves up and down at the voltage in the sea water, such as when welding is carried out, and all electronics moves up and down with it but there is no differential current injection because no taps are taken from the outer ground planes to the circuitry except at the ground star point.

All components, where possible are SMT. Lead free process is used. The cards and the components are all RoHS compliant, except for the oxygen cells which are shipped separately. The pcbs are US Underwriter Labs (UL) compliant FR4.

All pcb layouts conform with the Quality Control system operated by Deep Life Ltd, certified to ISO 9001:2000, including design for manufacturability rules, with 100% flying probe test.

[1] The field densities are sufficient to strip the chrome from brass regulators.

4.2 Component Screening

All component types used in the circuits have been screened for helium compatibility, to 140 bar.

All components have been screened to ensure none are obsolete, all comply with the CE RoHS Directive, and none are newly introduced.

All components that have reported reliability issues have been thoroughly investigated. This applies particularly to the oxygen sensors, pressure sensors, temperature sensors and connectors: all issues have been resolved or managed within the design.

4.3 Scrubber stick, 21-3-2007 13:28, Rev C

The scrubber stick provides secondary safety data, with multiple redundancy. For example, the risk of CO2 breakthrough is monitored using both a CO2 sensor and by monitoring the behaviour of the scrubber. Risks which are very low, such as CO or HC contamination, are monitored with a single sensor but that sensor is tested during start up.

Scrubber Stick, Page 1: Index

The circuit diagrams are organised as:

Page 1: Table of Contents

Page 2: Temperate Sensors

Page 3: Differential pressure sensor, gas temperature sensor, open scrubber Hall sensor, carbon monoxide sensor and connector to Base Unit

Page 4: Power supplies to infra red source and sensor

Page 5: Helium sensor

Page 6: Voltage references and ADC

4.3.1 Page 2: Temperate Sensors

Twelve temperature sensors are used to provide data which along with flow, pressure, ambient temperature and gas composition data, is used to monitor the health of the scrubber. The sensors are LM61 parts, which have proved rugged in test. The output from these sensors is a voltage, which is then multiplexed by two analogue multiplexers, with sharing of lines such that if one goes down, six temperature sensors are available.

4.3.2 Page 3: Differential pressure sensor, gas temperature sensor, open scrubber Hall sensor, carbon monoxide sensor and connector to Base Unit

U5 is a digital absolute pressure sensor that is used to provide redundancy of pressure data. The other absolute pressure sensors are on the sensor card, in the Base Unit, within the hermetic volume, and in the handset. Normally onto two of these sensor positions are populated. U5 has a limit of 14 bar, so is not fitted to units configured for commercial diving, or the data from them is not used: the sensor is not protected from helium offset drift in any case. U5 is intended for sports and special applications use only.

U12 is an analogue differential pressure sensor, measuring 0 to 1 bar. The normal operating range of this sensor is 0 to 5mbar, as it measures the pressure differential across the scrubber, to provide breathing rate and tidal volume data. This data is used for respiratory monitoring and to monitor the scrubber behaviour (scrubber health). This is a rugged capacitive ceramic sensor that has been tested in helium to 140 bar.

U7 is an internal gas temperature sensor, measuring the outlet gas temperature from the scrubber. The data is used to correct for CO2 absorption, to compensate for the reduction

in CO2 molecules in the measurement path as a function of the thermal expansion of the gas. This uses a LM35 precision sensor: this has much better linearity than the LM61, at four times the component cost.

U9 is a digital Hall sensor used to detect when the scrubber cap is open, so that if the pressure is close to 1 ATM, and the oxygen cells show a range compatible with that of air, then the sensors are calibrated automatically, with prompt to the user to refuse the calibration. The sensor also detects that the scrubber is properly shut during diving.

U35 is a carbon monoxide sensor with a special treatment by Aktina Ltd, to increase the sensitivity to both CO and HC, and reduce the response time. The sensor is used intermittently, due to its high power consumption, and the hot sensor emits infra red which can influence infra red absorption readings. It is installed on the opposite side of the board from the infra red sensor to minimise these effects.

The connector J1 is a hard gold plated male 0.1" pin array plugging into a female DIN 41612 connector on the sensor card that has bifuricated hard gold (non-porous) contacts. When not in use, the female connector should be protected by a dummy male connector. The DIN41612 connector has been found to be highly reliable, with over 30 years of experience with these connectors generally, and 6 years in a marine environment.

The circuit surpasses the requirements for ALARP.

4.3.3 Page 4: Power supplies to infra red source and sensor

U11 takes 7.2V power from the selected battery and steps that down to 1V for the infra red source, LAMP2, which is a micro machined silicon device.

U16 is a DAC powered from a 3V reference signal, the output voltage from which enables the infra red source to be modulated to maintain constant infra red power.

There are two measurement circuits, formed around U3, a dual ultra low drift chopper stabilised amplifer (AD8629). The first measures the voltage applied to the infra red source, and the second measures the current flowing through the infra red source.

There are two positive and two negative power supplies, for the infra red sensor mezzanine card, one set for the sensor itself and one for the buffer-amplifiers on the card. These are very low noise linear regulators due to the power noise sensitivity of these circuits.

The circuit surpasses the requirements for ALARP.

4.3.4 Page 5: Helium sensor

The helium sensor is used to compensate for noble gas spectral broadening of the CO2 measurements, and to compensate for gas thermal capacity in the scrubber health monitoring. A further application of the data from this circuit is to calculate precise decompression profiles, and to warn of excessive nitrogen pressures in the loop.

The sensor heater is based on a R45 (33 Ohms) resistor, which is heated to 80C for helium measurement. The helium level is measured once per minute, under control from the Base Unit.

Failure of the heater or the sensor results in a large change in the received data, which is detected. The system then assumes the worst case gas mixture for scrubber life, CO2 correction and decompression. This is a firmware requirement.

The circuit surpasses the requirements for ALARP.

4.3.5 Page 6: Voltage references and ADC

The voltage reference U21 is a very high precision and stable reference, which is buffered by U8, an ultra low drift chopper stabilised amplifier, which provides the references to the

ADC. The ADC is a 24 bit Sigma Delta device with perfect linearity, with variable over-sampling rates.

The buffer amplifiers for the ADC, U34, are also ultra low drift, low noise devices. These are in the same package as they operate on a differential signal, so the latent drift is removed. The bandwidth of the input signals to the ADC is controlled at source: the temperature sensors are inherently slow, and the amplifers buffering other sensor signals, such as U3 on the infra red sensor mezzanine card have filters to ensure there is no signal presented to the ADC within several decades of the Nyquist frequency of the ADC. The ADC acts as an integrator and has a 7^{th} order filter to reject out of band noise.

Failure of the ADC does not cause a catastrophic loss of data: only CO2, CO and HC data is lost. The temperature data, helium, differential pressure data is passed to the Base Unit and is measured by the ADC connected to the microcontroller, which then switches in as a guardian. There is thus dual redundancy on the safety critical functions. Loss of CO2 data is annunciated with messages to abort the dive, though there should be no immediate direct hazard because the scrubber health continues to be monitored.

The circuit surpasses the requirements for ALARP.

4.4 Infra-red sensor mezzanine card, 21-3-2007 13:28 Rev B

There are two mezzanine cards, one for CO2 only, the second for CO2, CO and HC.

The infra sensor is protected from pressure. It is exposed to 140 bar during testing. The pressure protective window has a full stress and displacement analysis published by the design team, with 400% safety margin on the deepest dive depth of 600msw. It is tested to 1200msw and analysed to beyond 2400msw. The risk is from failure of the rear of the sensor, which is epoxy filled for protection over and above that provided by the case.

All channels in the sensor are buffered internally, and all are buffered externally to increase the SNR from the mezzanine card to the scrubber stick. The external buffers are ultra low drift, low noise, chopper stabilised amplifiers. The bandwidth of the amplifiers is limited to prevent out of band signals being presented to the subsequent ADC.

The connector is formed from pcb solder pads: there are no mateable connectors. The noise is limited to signals traveling from an inner layer to the pad, then pad on the receiving side to the scrubber stick pcb. The pads are guard ringed with ground.

The circuit surpasses the requirements for ALARP.

4.5 Sensor card, 23-3-2007 11:23 Rev C

The card has only resistors, connectors and two sensors: optional digital pressure and optional humidity sensor.

The card connects directly with four oxygen sensors, type PSR-11-39-DL. These have an SMB male connector, which always mates with the ground before the signal to prevent ESD. These are routed differentially, with switches to ground in the Base Unit. When no sensors is installed, one line is connected to a DAC and the other to ground. The lines are routed with high inductance on an inner layer, and lump capacitances, to provide 25KV HBM ESD protection. There are also filters on the input to the ADC on each line of the differential pair of oxygen sensor lines.

Resistors R7 to R10 are to terminate the open drain digital Hall sensors to detect position of the automatic loop shut off valve.

Resistors R5, R6 and R3, R4 form the voltage divider to normalise the voltage out from the linear Hall sensor used for the position of the gas injectors, to the level required for the ADC.

Solder pads are used for connectors where at all possible. There are no Molex or pin type connectors except for the scrubber stick connector, which is a female DIN 41612 connector considered in the scrubber stick circuit.

Connection to the gas injectors is by hard wiring, using Kynar coated wire. There are no PVC coated wires in the entire system.

The circuit surpasses the requirements for ALARP.

4.6 Base unit card, 28-3-2007 8:28 Rev C

4.6.1 Page 1: Index

The circuit diagrams for the Base Unit card comprise 22 pages, as follows:

Page 1: Table of Contents

Page 2: Main and Aux battery switches

Page 3: Handset Battery Switch

Page 4: Charger, and battery current consumption monitor

Page 5: Voltage references and FPGA ADC1

Page 6: FPGA Analogue MUX and FPGA ADC 2

Page 7: Voltage references and MCU ADC 3

Page 8: MCU Analogue MUX and MCU ADC 4

Page 9: Oxygen sensor signal conditioning and voltage monitors

Page 10: FPGA supplies, FPGA Bank 0 and programming voltage supply

Page 11: FPGA Banks 1,2 & 2MB Serial EPROM for log storage

Page 12: FPGA Banks 2,3 & MCU Aux, MCU supplies

Page 13: MCU Ports 0,1

Page 14: MCU Ports 2,3

Page 15: Clock logic

Page 16: Redundancy switching logic for FPGA or MCU failure

Page 17: Power converters and linear regulators

Page 18: Connectors

Page 19: Optical fibre and LED drivers

Page 20: FPGA Oxygen Injector Motor Driver

Page 21: MCU Oxygen Injector Motor Driver

Page 22: Loop Shut Off Valve Motor Driver

These sheets are considered in turn.

4.6.2 Page 2: Main and Aux battery switches

Power is usually the Achilles heel for electronics: if there is power, electronics can be made extremely reliable, but the power systems themselves have a low MTBF. To manage this, layers of redundancy and monitoring are used. This complexity results in a reduction in MTBF, but a huge increase in MTBCF. This circuitry covers Pages 2 to 4 inclusive of the Base Unit circuit diagrams.

Each Base Unit has three power sources:

1. Main
2. Aux
3. External: This is from the handset in the case of the Sports unit, and from the MUX unit for the Commercial diving configuration. Note this is not umbilical power: it is not 24V. The MUX box takes the umbilical power and drops it to 5V5.

For the Sports unit, the power priority is as follows:

1. Main power
2. Aux power, if Main is lost
3. External power, from handset, if Main and Aux is lost.

For the commercial unit, the power priority is different, as follows:

1. External power
2. FPGA power, if External is lost.
3. MCU power, if External and Main is lost

Each power source is completely independent: they are in different physical containment and cannot be brought down by a single point of failure outside the Base Unit.

The single point of failure is a short circuit in the Base Unit: if this happens, it will load the power supply until it fails. To mitigate this risk, the FPGA and MCU have independent power supplies, so if one side develops a short circuit, the power supply can shut down and not bring down the whole system. As a further measure, all components that fail preferentially as short circuit have been eliminated from the design, such as tantalum capacitors.

External power circuits are on Page 3.

Main and Aux power circuits are on Page 2. The circuits include charger switches, battery switches (to switch out a failed battery). Current monitors are on Page 4.

Main power comes into the Page 2 circuit, and can be charged via the arrangement involving dual FETs, M8, switched by M1. The two series FETs reduce the risk of single FET failure bringing down a battery and also removes the leakage current via the internal FET diodes. M1 is controlled by either the MCU or the FPGA. That is, either of these can activate charging. There is a feedback line via R26 and R10 so both MCU and FPGA can check the action. R26 and R10 prevent a fault in either the MCU or FPGA from affecting the correct reading: it is high enough to prevent either circuit forcing a current into U1 sufficient to change the apparent logic state.

The same approach is used in all the switches and external peripheral control, where both FPGA and MCU may take an action. This approach meets the ALARP principle for SIL 4.

The same circuitry as used for switching between batteries, using M7, except that the XOR gate is powered from the Main battery instead of the post-redundancy power source. This allows either the MCU to power down the Main power source. The risk of a fault in the MCU causing the MCU to execute the program to power down the Main power is eliminated by having the FPGA monitor the state of the XOR U5, with active Brown out detection via R101 and R102, allowing both MCU and FPGA to power on the Aux power. If this is not executed in time, both will power down, the inputs to the XOR gate will fall to 0, so Main and Aux power will be off, but the External power will come on as U37 has a bias on its inputs. This then allows both MCU and FPGA to take the corrective action.

This is a very sophisticated power management scheme, that exceeds the ALARP requirements for SIL 4.

U2 is a Data Over Power transceiver that provides power from Main and Aux to the handset, along with redundant data (the primary data being communicated optically). If the handset is unplugged, or MUX is disconnected and the connector not capped, then there is a short circuit on the outputs of U1 (as sea water is highly conductive). This will take down MCU power, and is protected by a current limiting resistor, with an additional voltage monitor. The current drain will not be a critical failure: the dive can in fact continue normally, but as the equipment has a failure it should signal a dive abort as it would be known what other failure might be following.

All the circuitry on this page complies with the ALARP principle for SIL 4.

4.6.3 Page 3: Handset Battery Switch

The jumpers formed using soldered in wiring, J2, J3, J8 and J21, J20, J9, is used to switch between the charging arrangements for the sport and commercial units, and connect the main battery pads to a connector to a MUX for the commercial dive unit.

The External power circuit has data stripped off of it, via U3, then passes to a high integrity power switch which are the same as for Main and Aux power except that the final XOR gate has the bias on it to prevent the entire unit powering down in the case of either the MCU or FPGA failing in a mode that turns off both the other power sources.

All the circuitry on this page complies with the ALARP principle for SIL 4.

4.6.4 Page 4: Charger, and battery current consumption monitor

The top half of this page is the battery charge regulator, taking 5V power and steps that up to 7V3 for constant voltage mode charge of Valence pure Lithium Ion gel batteries. The batteries are charged in two stages: first constant current, at 600mA, then constant voltage, in line with the manufacturer's guidelines. On battery pack at a time is charged, with the Main battery first, then Aux, then Handset (if it is connected). The charge state of each battery is monitored.

The regulator taking the charger power source from 5V to 7V3 is U70. The power source is a Nokia phone charger, or equivalent source generated from umbilical power in the MUX for the commercial dive unit.

In the commercial dive unit, there is no current limit to the umbilical power, so the FPGA and MCU are able to switch on the charger for both batteries simultaneously, on demand.

The charging monitor is formed by U14, but this requires a power voltage double that being monitored, so 14V is generated using U32 but at very low current.

All charge circuitry is off until charge power is applied: this means the circuitry is off almost all the time for the Sports unit, but for the Commercial unit it can be switched on at any time, under control of the FPGA or MCU via the ON_Charger supply to U70. The arrangement with U14 being powered from the charge source, and U70, prevents incorrect operation of the FPGA or MCU switching the supply on inadvertently in the Sports unit if no charger power is available.

The current sensing for all power drawn from the selected power source is measured using U8. This allows the MCU and FPGA to detect an abnormal load, as well as monitor the current consumption of the unit as part of the continuous self test regime.

The feedback from the charger to the MCU and FPGA are via R55 to R67 resistor set: these are individual to the MCU and FPGA to prevent a short on MCU/FPGA, from affecting the result in the FPGA/MCU.

The FGPA and MCU have control over the charger via XOR gates U88 and U89.

All the circuitry on this page complies with the ALARP principle for SIL 4.

4.6.5 Page 5: Voltage references and FPGA ADC1

There are two ADCs that read the various sensors and monitoring channels for the MCU, and a further two for the FPGA. This means that if the MCU or FPGA goes down, the data is available to the part of the system that remains up.

There is a further subdivision of the ADCs, such that each of the MCU and FPGA can read all oxygen sensors, but if an oxygen sensor with a very high voltage output is connected, such as occurs when the sensor's internal load resistor is open circuit prior to the sensor being plugged into the electronics, then it will destroy only one ADC and there are still two oxygen sensors that can be read from the other ADC.

The FPGA can read all data on the MCU ADCs, and visa versa, using a serial data exchange between the two units: there are actually two serial interfaces for redundancy even though this is not a safety critical function. One interface is via I2C, the other is a simple asynchronous RS232 like serial interface. There is also a JTAG interface between the two, but is used only for configuration upload to the FPGA via the MCU USB interface when the unit is not in operational service.

The precision and high stability voltage reference for the FPGA ADCs is formed using U74, with almost zero drift chopper stabilised buffers U15.

The first ADC for the FPGA is U71. All ADCs in the system are the same: 24 bit Sigma Delta with integral 8 input differential MUX. All data is routed as differential signals to reduce noise and increase noise immunity. The ADC uses low noise external buffers, U79, which is specially designed for capacitive loads and recommended by the ADC's Design Authority.

The ADC is powered from 5V, and the output from the ADC is reduced to 3V3 for the FPGA using a zener via R193.

All the circuitry on this page complies with the ALARP principle for SIL 4.

4.6.6 Page 6: FPGA Analogue MUX and FPGA ADC 2

This is the same as for Page 5, except there is a MUX formed by L24, and an ambient temperature sensor U53. This sensor has a very slow response, as it is in the same silicone oil as the Base Unit: it is intended for use in the commercial dive unit in a saturation environment only.

4.6.7 Page 7: Voltage references and MCU ADC 3

This is the same as for page 5, except it is for the MCU instead of the FPGA.

4.6.8 Page 8: MCU Analogue MUX and MCU ADC 4

This is the same as Page 6, except it is for the MCU instead of the FPGA, and there is no duplication of the ambient pressure sensor.

4.6.9 Page 9: Oxygen sensor signal conditioning and voltage monitors.

The oxygen sensor signal conditioning on this page comprises a set of DACs: the inductance and capacitance to enhance the ESD protection is on XXXXXX.

4.6.10 Final Review

The remaining circuits have been reviewed and appear clean, however these should be reviewed again with a larger review team before the project complete the NORSOK requirements (that is, changes done for five units for NORSOK). That review will cover:

- Page 10: FPGA supplies, FPGA Bank 0 and programming voltage supply
- Page 11: FPGA Banks 1,2 & 2MB Serial EPROM for log storage
- Page 12: FPGA Banks 2,3 & MCU Aux, MCU supplies
- Page 13: MCU Ports 0,1
- Page 14: MCU Ports 2,3
- Page 15: Clock logic
- Page 16: Redundancy switching logic for FPGA or MCU failure
- Page 17: Power converters and linear regulators
- Page 18: Connectors
- Page 19: Optical fibre and LED drivers
- Page 20: FPGA Oxygen Injector Motor Driver
- Page 21: MCU Oxygen Injector Motor Driver
- Page 22: Loop Shut Off Valve Motor Driver

5 CIRCUIT REVISION D

The Revision D circuit is correction of circuit deficiencies in the Revision C samples, found by application of a SIL 4 rigour throughout an extensive verification process, involving involved 16 samples, literally thousands of chamber runs, over a hundred manned dives, comprehensive formal modelling, in addition to bench validation tests.

Each of the issues found were documented using the Mantis and Engineering Change Order systems applied to track non-conformances by Deep Life Ltd. They are captured here to record permanently these upgrades, in a form readily accessible to future reviewers, or to staff proposing modifications to the electronics.