DEEP LIFE OPEN REVOLUTION FAMILY OF REBREATHERS

Failure Mode, Effect and Criticality Analysis Volume 8:

Rebreather to Umbilical Communications Circuits

DOCUMENT: [Filename]	FMECA_OR_V8_Elec_MUX_080304.doc
ORIGINATOR:	**Dr. Alex Deas, Igor Abrosimov, Marat Evtukhov**
DEPARTMENT:	**Engineering**
UPDATED:	**4th March 2008**
REVISION:	**C1**

APPROVALS	
_AD_____ Project Manager	_____ Date
_VK_____ Quality Officer	_____ Date

Controlled Document ☒ Classified Document ☐

DO NOT COPY.

Revision History

Revision	Date	Description
A	5th Dec 2007	Review of Rev C Circuit
B	17th Jan 2008	More details of Rev C Circuit review
C1	10th July 2008	C0 4th March 2008: Include feedback from review of this document. C1 after further review of actions and effect of removing optics

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 Volume 8 of the FMECA of the Deep Life Open Revolution Submission, covering the communications multiplexer in the surface supplied version rebreather, i.e. with umbilical gas, power and comms.

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 MUX unit has been formally assessed as SIL 2.

2 CIRCUIT REVIEW OF UMBILICAL TERMINATOR

2.1 Naming

The first question is “what is this board called?” Historically the board has been called the “MUX” (abbreviation of Multiplexer, as at the beginning of the project that is all the board had to do), but in fact it is now an Umbilical terminator. Keeping the historic name risks confusion with the “Micro-MUX” which is a true MUX-DEMUX device forming a mezzanine board that fits to the Umbilical terminator.

Action: Rename all project related files “Open Revolution Umbilical Terminator”. For abbreviation, the “UT”.

When implementing this tidy up, the project files should be made to comply with QP-26.

2.2 Revision

The circuit reviewed carries a date stamp 17th September 2007, and is marked Revision C.

2.3 Functionality

The Umbilical terminator provides the following functions:

1. Multiplexing and demultiplexing of data up and down umbilical media.
2. Support for a media interface board, normally a Optical Micro-Mux, to a corresponding Micro-MUX board at the other end of the umbilical.
3. RS485 bidirectional data transfer to a corresponding MUX board at the other end of the umbilical.
4. Framing protocol to pack and unpack the data
5. Digitally programmable and monitored power control for lighting, cameras, heating and rebreather
6. Data routing hub with port to rebreather, head up display or PFD, using RS485 and optical links in a redundant configuration
7. USB controller
8. Digital / analogue audio system interface for microphone and speaker between diver and topside.

9. Safety monitors: flood sensor, diver emergency sensor, helmet closure sensor

2.4 Safety Architecture

The board is designed to be dual redundant, with outputs split such that the failure of one channel is not a critical failure: for example, the suit heaters are assigned to different channels, the two cameras are served by independent channels, etc.

There is concern that two different FPGA configurations are used for the Top Side use of this board and the Rebreather side. This doubles the amount of work, and the risk of errors – they are connected in series not in parallel (which would reduce point).

Action: IA is leading a rewrite of the FPGA code, to use a single FPGA load into all devices. Once this achieves the same functionality as the existing development, then the current development will be stopped and forward development will use the integrated architecture.

Action: The PCB should be revised at the next opportunity to use the same pin out, and to ensure there is a single function per pin. To achieve the latter the front panel connections require their own pins rather than reuse pins: this involves just 3 extra pins! This would also simplify field stocking because the same board could be used to replace a Topside Unit (TU) Umbilical Terminator card or a Rebreather Side UT.

Action: There are inadequate test harnesses. Additional harnesses should be put in place, to form both a structural (module) level and behavioural (system) level test benches.

2.5 Page 1: Table of Contents

The table of contents lists 22 pages and the structure seems reasonable.

Action: The date is in the wrong format. Change system settings to correct.

2.6 Pages 2 and 3: FPGA1 and FPGA2 Power Supplies

Each half of UT is powered by separate power supply to achieve the SIL 2 MTBCF target for this system.

The unit is powered from a nominal 24V. This concurs with a review by the client in November 2007. The actual supply may vary from 12V to 30V.

The regulator part is the LT1374HV version, which has an absolute maximum of 32V.

The LT1374HV operates at a fixed 500KHz switching frequency, and with the resistors used in the circuit it will produce just below 6V worst case.

There are no electrolytic capacitors or tantalums, as these would cause the circuit to immediately fail the MTBCF target (both fail short, when explode with the energy involved). Ceramic capacitors are used in their place: this is good design practice – the ceramic capacitor tends to fail gradually – one leaf at a time, and open circuit rather than closed.

Action: Put voltage ratings beside all of the ceramic capacitors if they need higher than 5V rating, just as the same way an electrolytic would be thus marked on a circuit.

Action: D8 and D24 do not seem to do anything useful, so remove them.

Action: the rating on D6 and D7 is a 30V diode, which is too close to the 30V input limit. D7 and D6 should be regular diodes instead of Schottky, as regular diodes are both cheaper and a lot more reliable.

Action: check C142 and C140, C135 and C136, can tolerate 30V. This is required if the first regulator stage fails.

Action: As data are not transmitted over power nets extra components connected to U62 and U63 shall be removed and U62, U63 shall be moved to page 21

Umbilical power supply is provided through 2x24V_IN and 2 ground terminals. There is only one current sense on page 2. Power contacts are paralleled but there is no means to check that both contacts are present. Diagnostics and self test functions may be substantially improved with independent current sensors per power contact.

Action: Consider adding 3 main power current sensors to have sensor per pin.

Action: Input under voltage and converter output under/over voltage comparators shall be added supplying FPGA and ARM microcontroller with power failed signals to allow them to enter power saving mode. It also needs to be checked that power saving mode achieves required 50mA maximum power consumption level for both halves of UT device.

2.7 Pages 4 and 5: ADC1/ADC2 and references 2.5V, 1.19V

Band gap references U7, U8, U22 and U23 are used to reduce maximum amplitude of the ADC data output (currently run at 1Mbps) and busy signals. This may cause incorrect data reading from ADC.

The 8MHz core clock to ADC is supplied through FPGA affecting measurement accuracy due to clock jitter. Input clock range for this ADC is from 0.1MHz to 20MHz. This ADC may be clocked by 12.288MHz clock instead of 8MHz clock eliminating the 8MHz clock source.

Action: Remove U7, U8, U22 and U23; Check minimum current consumed from 3.3V and if it is less than possible leakage through FPGA ESD diodes then put resistor between 3.3V rails and ground to pass required amount of current.

Action: Connect clock directly to 12.288MHz crystal oscillators.

2.8 Pages 6 and 9: FPGA1/FPGA2 configurator, FPGA1/2 bank 4

The 2.5V decoupling capacitors are spread across 2 pages each page having both “left” and “right” halves caps while according to the pages name they supposed to be on proper pages.

Configuration EEPROM shall be connected to one FPGA for configuration purposes and to another FPGA for programming EEPROM purposes. At the moment programs its own EEPROM making reprogramming not tolerant to programming errors.

Action: Sort out capacitors between pages 6 and 9.

Action: Pass EEPROMs U80 JTAG port to the USB port controller (a LPC2478 ARM microcontroller) for EEPROM programming through USB port.

2.9 Pages 7 and 10: USB TRANCEIVER1/2, FPGA1/2 banks 0, 1, 2, 3

USB ports do not have proper pulldown/pullup resistors to provide an ID: it is implemented as reworks in current version.

There are no pullups/pulldowns on HELMET_CLOSED and CHICKEN_SWITCH nets which is suspicious. As these inputs are not used any more it is suggested to remove them.

On page 10 12.288MHz and 8MHz clock signals are connected to FPGA2 pins which are not capable to drive internal clock resources through dedicated clock trees. It is also more reliable to use external 48MHz external crystal oscillator to supply clock to FPGAs instead of multiplying it by 6 internally inside FPGAs.

USB interface implementation is not compatible with some available host controllers. While extra efforts in debug are required it is difficult to have the current implementation completely debugged because the number of possible host controllers is virtually unlimited. It is proposed to solve this by replacing the FPGA USB controller by a USB controlled built using an LPC2478 ARM microcontroller. Integrated clock synthesiser into LPC2478 device

allows using single 12.288 MHz clock source and thus extra 48MHz clock source is not required for the second half of UT.

LPC2478 ARM microcontroller shall use one USB port to connect to USB HUB for diver side UT version and use second USB port for direct external connection to PC for top side UT version to provide dual redundancy for the segment between PC and UT.

Objections are raised on this proposal by Verification, claiming it would be too difficult to verify the software code, and a completely code-less system should be maintained. In this case, the ARM processor will act only as a USB port: this is what is used now.

Action: Update schematics with USB transceiver reworks.

Action: Check whether any pullups or pulldowns are necessary on HELMET_CLOSED and CHICKEN_SWITCH nets.

Action: Consider whether to replace FPGA2 with LPC2478 ARM microcontroller. Note: this was done and was rejected – the current architecture appears to be the safest and avoids all software.

Action: Add 48MHz clock oscillator.

2.10 Pages 8 and 11: Audio Codec 1/2, FPGA1/2 banks 6, 7, 8, Fibre interface

Audio codec AD74111 provides only 11 valid bits at 48kHz sampling rate in typical case which is insufficient accuracy for further spectrum correction. It is proposed to use ADC WM8786 and DAC AD1955. This may improve overall accuracy to 18 valid bits level. To achieve this it also requires direct connection between DAC/ADC and 12.288MHz crystal oscillators.

Alternatively two different halves of UT may use different audio codecs to reduce systematic failure risk.

2.5V decoupling capacitors C68, C146 and C147 are placed on wrong pages.

Optical receivers provide TTL levels on their outputs and there are band gap reference components which limit signal amplitude to 3.3V level. Turn on time of this component is about 100us at 150uA operating current. This exceeds one bit interval and may take even longer as current itself is hardly predictable.

SCRUBBER_HEATER_LEFT_OFF and SCRUBBER_HEATER_RIGHT_OFF are implemented incorrectly. First they are used as bidirectional while input voltage range does not match receiver thresholds. Secondly if one FPGA is powered down due to power supply failure it will shut down heaters in both channels through ESD diodes. Thirdly power up state of this signals have wrong polarity, i.e. they shall be powered up having active 0 on this bidirectional pins.

FPD interface needs dedicated FPGA pins allocated to this interface.

Action: Replace audio codec.

Action: Move decoupling capacitors to the right page.

Action: Remove band gap reference components U35 and U37.

Action: Correct SCRUBBER_HEATER_LEFT_OFF and SCRUBBER_HEATER_RIGHT_OFF implementation using extra components such as transistors/diodes/resistors.

Action: Add PFD interface.

2.11 Page 12: USB HUB and clock oscillators

Main clock source for FPGAs shall be 48MHz as mentioned in 2.9.

Mentioned in 2.9 USB ID related reworks may affect this page.

2.12 Page 13: Cameras power supplies

These power supplies operate from 24V power supply input and thus have the same issues with Schottky diodes as described in 2.6.

Power supplies are controlled using direct connection to FPGA pins which causes wrong polarity of control signals at power up. It needs mosfets (same type as M1) to invert polarity.

Inductors L7 and L8 does not indicate on the schematics value and current rating.

Current limit resistors do not correspond to the output current rating.

Action: Change type of D11 and D12.

Action: Check voltage rating for capacitors on the input and output.

Action: Add transistors to invert DC/DC converters shut down control signals.

Action: For all inductors put value and current rating on the schematics.

Action: Add current rating for each power supply output on the schematics and check current limiting sensors.

2.13 Page 14: Lights power supplies

Same comments as in 2.12

Action: Actions from 2.12 with corresponding reference numbers.

2.14 Page 15, 16 and 17: Scrubbers', Legs & Arms, Gloves and Torso Heaters power supplies

Same comments as in 2.12. It may need more transistors in shut down control network if they shall be controlled from either FPGA.

For heaters' power supply it may make sense to consider using whole 24V amplitude applied to the heaters with sigma-delta controller implemented inside FPGA replacing this DC/DC converters with MOSFET switches.

Action: Actions from 2.12 with corresponding reference numbers.

Action: Consider alternative heaters control mechanism.

2.15 Page 18: Heater suit current sensors

In case alternative heaters control is used this page may need changes to check current sensing is correct.

2.16 Page 19: Prizm muxes power supplies

There is no need for these power supplies as DL MICROMUX modules have their own DC/DC converters

Action: Remove these power supplies.

2.17 Page 20: Audio amplifiers

Linear output must be buffered by AD797 to avoid audio performance degradation in the link to spectrum correction equipment. At the moment signal is supplied unbuffered.

AD620 amplifiers are not specified for audio applications and have a large noise level. Amplification ratio is also far from optimal. With MSM2C microphone for -22dB version the output voltage is 1.6mV RMS assuming 2×10^{-2} sound pressure. To interface with WM8786 G=1000 shall be used.

Action: Buffer linear outputs and replace input amplifier with AD797 or similar amplifier correcting amplification ratio.

2.18 Page 21: RS485 Transceivers

There are two types of RS485 transceivers used across this design: SN65HVD10D (32Mbps device) and LTC1480CS8 (2.5Mbps device). They may all be replaced with SN65HVD11D 10Mbps chips having less noise in the links and less number of different components.

Couple of transceivers shall be moved from pages 2 and 3 into this page.

Action: Change type of RS485 transceivers.

3 REMOVAL OF OPTICAL LINKS

3.1 Upgrades resulting from reduction in redundancy

Following evaluation of 5 rebreathers in Bergen in May 2008, it was decided to remove the micro-muxes from the UT, locating them in a Bell commutator box instead. This reduces the reducancy from quad to dual, and reliance on electrical twisted pair signals.

To off-set the increases risk, all twisted pair channels were upgraded from a 4KV HMB ESD resilience to 50KV ESD and 70VDC common mode, by using 16KV transceivers and spark gaps. Furthermore, all video signals were made fully differential and isolated using video transformers. All helmet connectors were upgraded to fully digitial, with replacement of the speaker and microphone circuits with a digital driver and receiver in the PFD Helmet Display card – a new card was designed, laid out and built.

A wiring board was created to hold this additional electronics in the UT which passed a clean review.