

Deep Life Open Revolution Family of Rebreathers

Design Verification Report: Rebreather Power Architecture

DOCUMENT NUMBER: DV_OR_Power_080319.doc
[Filename]

ORIGINATOR: Dr. Alex Deas, Igor Abrosimov, Dr. Sergei Pyko,
Dr. Sergei Malyutin

DEPARTMENT: Verification

DATE UPDATED: 19th March 2008

REVISION: A2

APPROVALS	
_____	_____
Hardware Architect	Date
_____	_____
Software Architect	Date
_____	_____
Project Manager	Date
_____	_____
Quality Officer	Date

Controlled Document

Classified Document

DO NOT COPY EXCEPT UNDER NDA.

Revision History		
Revision	Date	Description
A, A1, A2	19 th March 2008	Document created 9 th March 2008 when it was recognised it was missing from the Design Verification reports for the umbilical to power switching functions. Updated with all reviewers comments on 12 th March 2008 to A1. Discussion with Design Authority, concluded 19 th March 2008

Copyright © 2008 Deep Life Ltd

All rights reserved. No circuit may be reproduced without a license for the topographical rights contained therein from Deep Life Ltd. This document does not constitute a license to use and patent, patent application or topographical right of Deep Life Ltd.

Table of Contents

1	PURPOSE AND SCOPE	3
2	SAFETY ASSESSMENT	3
3	OVERALL POWER SUPPLY SCHEME	3
4	SWITCHING BETWEEN SUPPLIES	4
4.1	Functionality of power switching.....	4
4.2	State Transitions in power switching	4
4.2.1	States.....	5
4.2.2	Pseudo-states.....	5
4.2.3	Transitions	6
4.3	Safety Backstop	7
5	RELIABILITY OF U30.....	7
5.1	Waveforms on U30 under minimum load conditions	8
5.2	Power Failures During Testing	14
5.3	Waveforms on U30 under full load (worst case conditions): SOV, 2 injectors, LEDs, Scrubber stick, speaker etc.	14
5.4	Independent review of U30 reliability	16
6	BATTERY HOUSINGS	18
7	CONCLUSIONS.....	18
8	ENGINEER CHANGE ORDER REQUIREMENTS	18
9	REFERENCES.....	18

1 PURPOSE AND SCOPE

The purpose of this document is to verify that the Open Revolution rebreather power supplies, including:

1. The overall power supply scheme
2. Current limits and their operation
3. How the rebreather manages failure and reinstatement of primary and secondary power, for example, of umbilical power and battery power.

This document does not cover the FMECA of the power components: this is handled in Volumes 2 and 3 of the FMECA for the products.

The scope of this document is a design verification of the Power Architecture in the Base_Unit circuit revision C1 according to QP-20.

2 SAFETY ASSESSMENT

The eSCR has been assessed at SIL-4 as a design in volume production. A single event on a single eSCR the Safety Integrity Assessment is SIL-3.

3 OVERALL POWER SUPPLY SCHEME

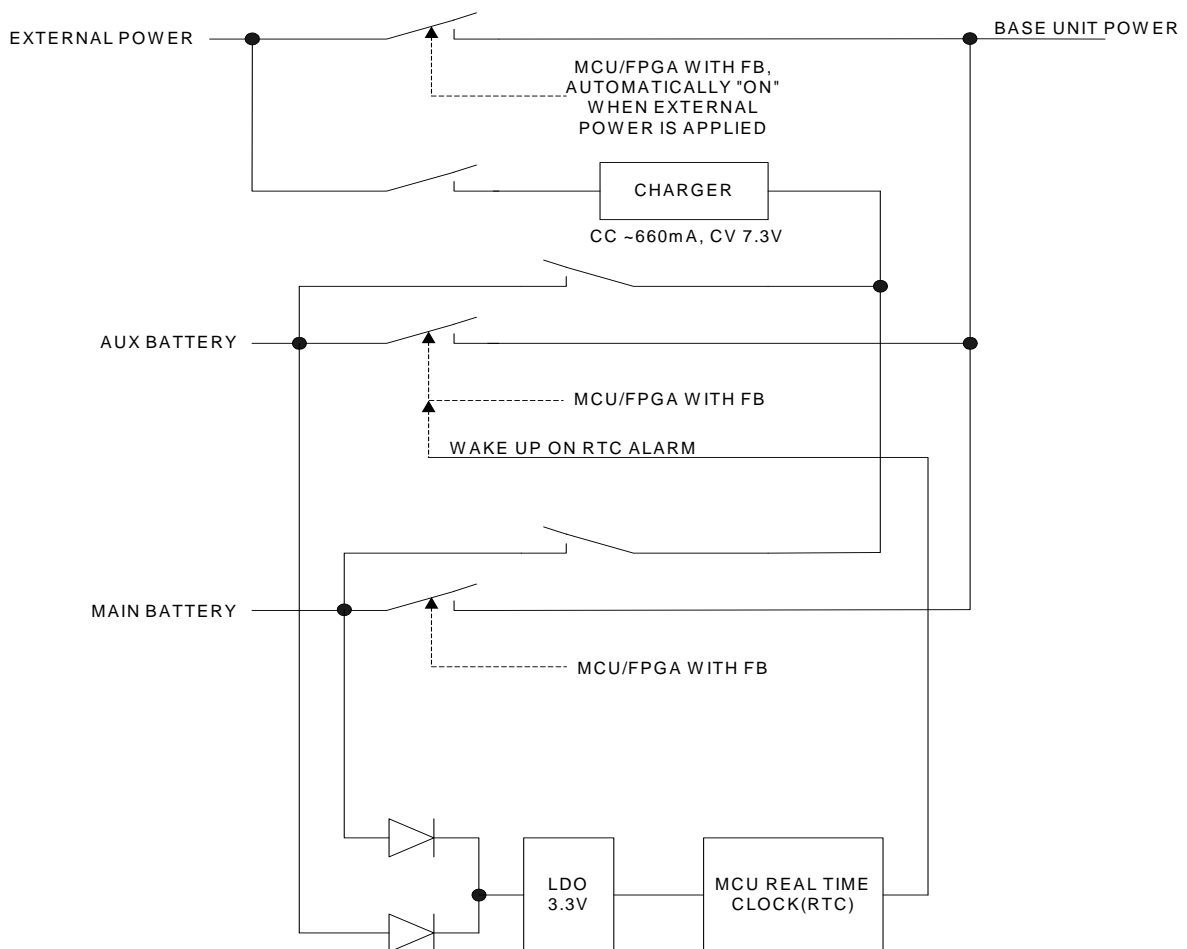


Figure 1: Base Unit Batteries Switches Block Diagram.

4 SWITCHING BETWEEN SUPPLIES

4.1 Functionality of power switching.

This section will focus on the case where primary power is from Umbilical power, regulated down to 5V3 and secondary power is the batteries. The same events occur with two battery sources, or handset power with backup local batteries: the exact configuration depends on the application.

The umbilical power supplied to the rebreather is a 5V5 supply: this is regulated down from main umbilical power by the Umbilical Terminator. The main umbilical supply can vary over the range 6V to 30V, and nominally 18V.

The rebreather is powered normally using umbilical power. There is a provision for battery power in case the umbilical power is lost.

The power on-off algorithm does not ever power down the unit whilst there is sufficient power for it to operate: the unit sleeps in a safety mode where every 10s it checks if the PPO2 has fallen significantly, and if so switches into a full powered up mode. These internal operating modes are outwith the scope of this report: this report focuses on the electrical functions of how power is applied, and what has to happen when it is lost.

The rebreather is normally never off: it monitors the PPO2 every 10s even in a sleeping state, and powers on if the PPO2 falls to dangerously hypoxic levels or if it detects breathing on the Rebreather from a fall in PPO2 over a short period of time. This algorithm and its verification is the subject of separate documents.

4.2 State Transitions in power switching

Consider this as a state transition diagram as shown below:

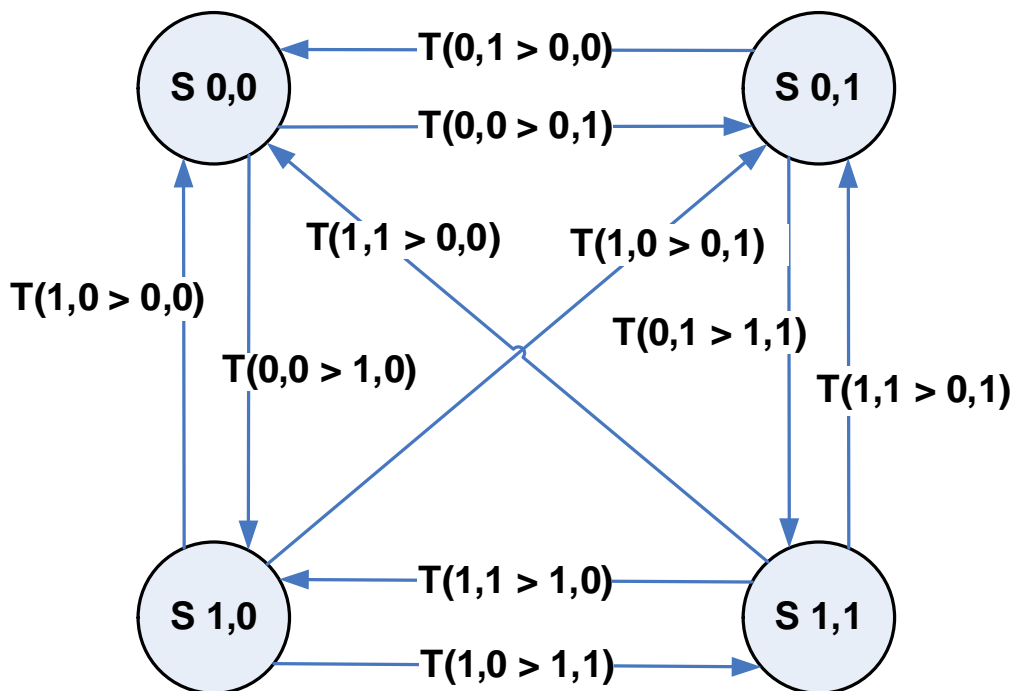


Figure 2: State-Transition diagram for rebreather power sources. State S x,y where x denotes whether there is umbilical power (0, or 1 as a binary parameter), y denotes whether there is battery power, also as a binary parameter.

4.2.1 States

The states are:

- **State(0,0)** is where the umbilical power is off, and battery power is off. This steady state is safe, in that it does not damage the electronics.
- **State(1,0)** is where the umbilical power is on and battery power is off. This steady state has been used extensively in lab tests, and has been reviewed. It appears to function correctly.
- **State(0,1)** is where the umbilical power is off and battery power is on. This steady state has been tested less extensively, but has been tested: it was demonstrated at DEMA and was used in the unit in St Petersburg for the trials to 5th March 2008. It appears to work.
- **State(1,1)** is where the umbilical power is on and battery power is on. **This is a fault condition: the MCU and the FPGA must follow the correct protocol, otherwise this fault condition will occur.**

The FPGA and MCU must prevent the equipment ever being in State(1,1), but it would be prudent to check the equipment is not damaged should the power supplies enter this state transiently due to capacitance etc. The way the equipment avoids this state is that when the umbilical power is applied after the unit has been running from batteries, the batteries will try and drive the umbilical. This is detected the lines “ON_HANDSET_BATTERY_FB_MCU” and “ON_HANDSET_BATTERY_FB_FPGA” on page 3 of the circuit diagrams: the names are a little misleading, as they date from the use of the handset to power the rebreather – the Top Side Unit and Umbilical Terminator are a substitute for the diver’s handset.

4.2.2 Pseudo-states

There is one more state which is similar to S(0,0) but can exist only for very short periods: it differs from S(0,0) in that there is sufficient charge in capacitors to operate for a short time. It may be considered as S(0,0+), and in this state S(0,0+) the MCU and FPGA are fully operating.

Transition from S(1,0) always goes to this state first and then from this state into S(0,1) when comparator detects low voltage in POWER_SUPPLIES node.

There is no direct path from S(1,0) to S(0,1) or visa versa, but transitions could exist theoretically.

The Base Unit does go from S(0,1) to S(0,0+) periodically, otherwise it cannot sense the presence of the main power source. If it is present then it goes from S(0,0+) to S(1,0) when the diode in the Umbilical Terminator starts passing current when capacitors at the POWER_SUPPLIES node are discharged to 5.8V or so. If external power is absent it then goes back to S(0,1) for a while and then back to S(0,0+). If batteries are discharged it goes from S(0,0+) to S(0,0) and turns off completely. As the Umbilical Terminator X source has a diode to prevent from sinking current, State (1,1) seems unreachable when batteries have a higher voltage than the Umbilical Terminator source. A state diagram in the attached file below original diagram.

When batteries are discharging it shall not leave state S(0,1) if the comparator sees the POWER_SUPPLIES node below the threshold to switch to a battery. Thus when batteries are discharging it goes to S(0,0) from S(0,1) directly, not through S(0,0+)

When the unit is turned off normally it shall go to S(0,0) from S(0,0+).

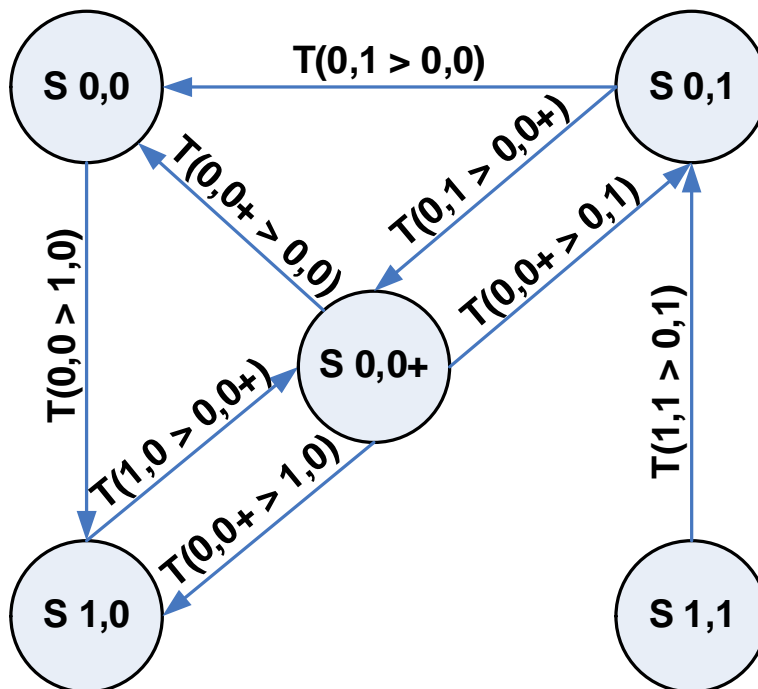


Figure 3: State-Transition diagram showing transitory state S(0,0+) and its links. All invalid transitions are excluded from this diagram, e.g. S(1,0) to S(1,1).

Instead of inserting an additional state, an alternative view is to recall that numbers in brackets actually denote the state of power switches, and the state S(0,0) means that both switches (umbilical and battery) are off. The device may shortly work in this state using the energy from the power supply decoupling and smoothing capacitors.

4.2.3 Transitions

The transitions are:

- To S(0,0) or to S(0,1) from first built, depending on the battery power level.
- **T(0,0 > 1,0) occurs automatically** (i.e. without MCU or FPGA intervention), if umbilical power is applied from the full power down state: the input to U37 from R95 on page 3 of the schematics is pulled up by umbilical power, if the MCU is not forcing it down. This then turns on the FETs M6 and M12, to supply power to the rest of the electronics from the umbilical supply.
- **T(0,0 > 0,1) is an invalid state: it should never occur.** The MCU or FPGA must be powered to switch on the battery power: if cannot do this if there is no previously existing power and no umbilical power.
- **T(0,1 > 0,0) occurs when the battery is exhausted.** The equipment receives a brown out signal, then should:
 - put the injectors into a safe state
 - tell the diver to bail out now
 - shut the shut off valve
 - power down.
- **T(0,1 > 1,1) is a momentary transition.** The real time counter is the only active function when the unit is in Zombie state: this might let the unit get into state S(1,1)

for 10s or more. As soon as the MCU of FPGA detect that the umbilical power is restored, the should switch off their battery power.

- **T(1,0 > 0,0) occurs when the umbilical power is being lost, but the equipment fails to apply batter power, due to the batteries being empty.** The equipment receives a brown out signal, then should try to take the same actions as for T(0,1 > 0,0).
- **T(1,0 > 0,1) occurs when the unit is running on umbilical power and receives a brown-out signal.** The MCU and FPGA must IMMEDIATELY switch on their battery power, otherwise the unit will totally power down.
- **T(1,1 > 0,0) is technically an invalid transition,** but occurs if there is a sudden catastrophic failure of primary power supply components.
- **T(1,1 > 1,0) occurs as a normal result** after transition T(1,1 > 1,1)
- **T(1,1 > 0,1)** occurs if there is a brown out while the system is in state 1,1

Note: An experiment should be run to determine from power measurements, how much time is actually available when there is a sudden and total loss of umbilical power, and also that the power switching to battery power does actually work with sufficient margin, under conditions of maximum power drain.

Under minimum load conditions the transition into state S(0,1) from S(1,1) state takes 110us; into state S(1,1) from S(0,1) state takes 130us, from empirical measurements.

In the sequential controller (MCU), the existing code uses switch overlap transitions, i.e. initially the new power source is loaded, and after that the defective power source is disconnected. This may have a drawback of a higher initial pulse current from the battery, however, it minimizes the chance of loosing control completely. The duration of this overlap is very small: about 100 uSec.

There are no direct transitions between S(0,0) and S(1,1) and between S(1,0) and S(0,1), except in theory (they are race hazard conditions): these transitions are in practice a two-step transition, since even in a parallel controller (FPGA) the on and off commutations have different durations, and the device reaches the target state through one of available intermediate states. The probability of T(1,1 > 0,0) and T(1,0 > 0,1) transistions is extremely low.

4.3 Safety Backstop

There is another pseudo event: the Real Time Clock is permanently powered from the batteries. It generates a battery on signal periodically. This guarantees that if the MCU or FPGA fails to turn on the batteries after a power failure, perhaps due to an exceptional fault current, then the RTC will turn them on anyway and give a regular wide opportunity for either the MCU or FPGA to restore permanent power.

5 RELIABILITY OF U30

During trials two cards failed, on two different rebreathers, due to a failure of U30: a MAXIM negative voltage converter and in another case, of a Linear Technology equivalent. This led to a check of the voltages on each pin of U30 using a scope, and an independent review of the circuits and their operation.

5.1 Waveforms on U30 under minimum load conditions

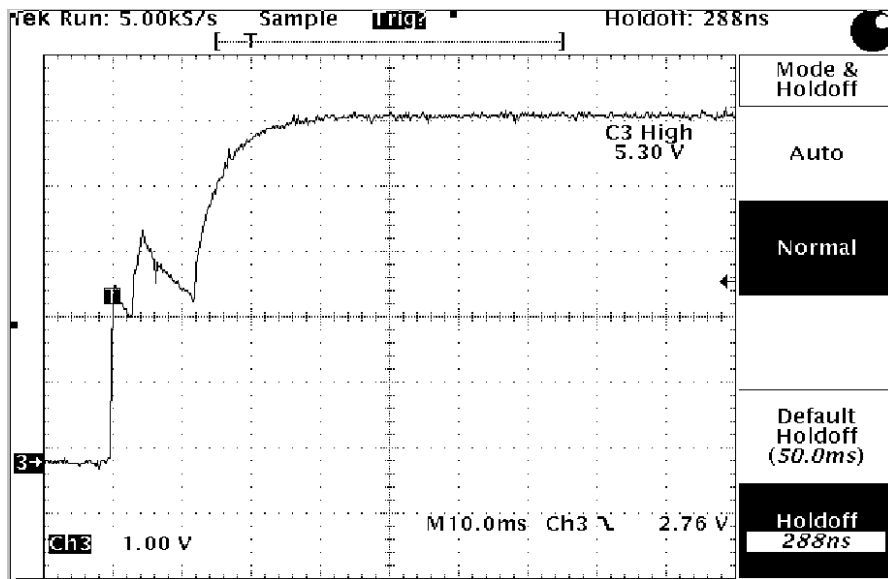


Figure 4. Pin8, U30 (Vin+). Umbilical Power OFF->Power ON, Battery is Off

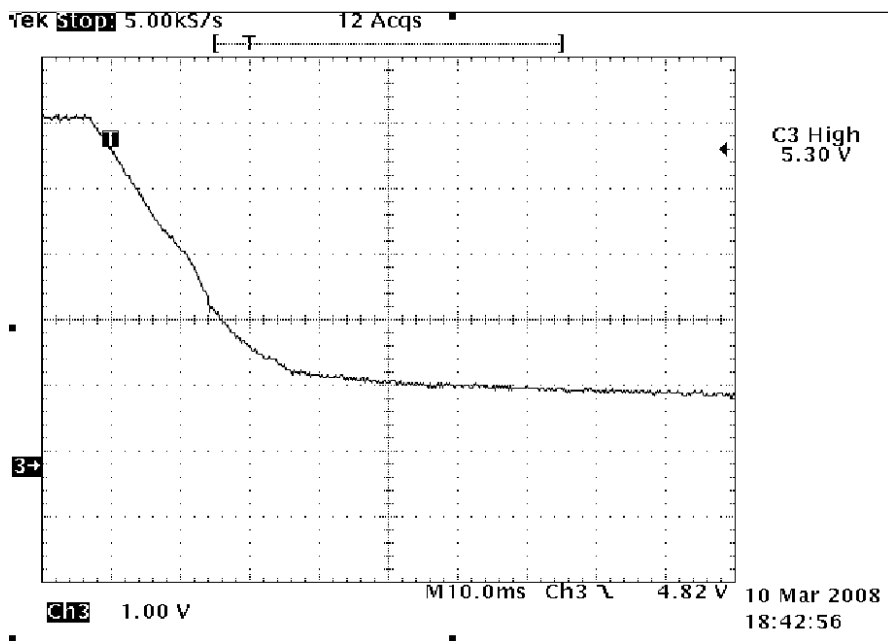


Figure 5. Pin8, U30. Umbilical Power ON->Power OFF, Battery is Off

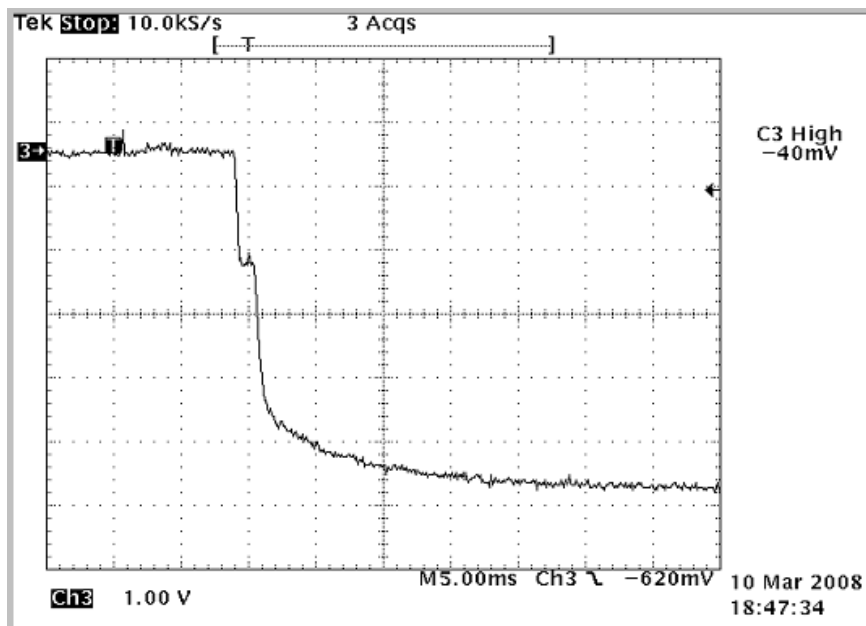


Figure 6. . Pin5, U30. Umbilical Power OFF->Power ON, Battery is Off

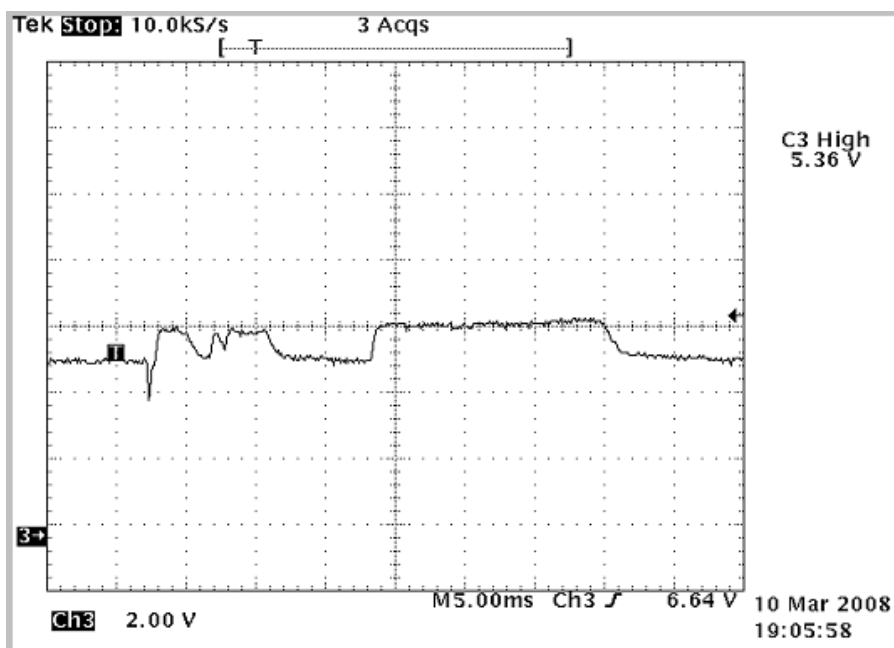


Figure 7. . Pin8, U30. Umbilical Power ON, Battery Off ->ON (with help the external jumper)

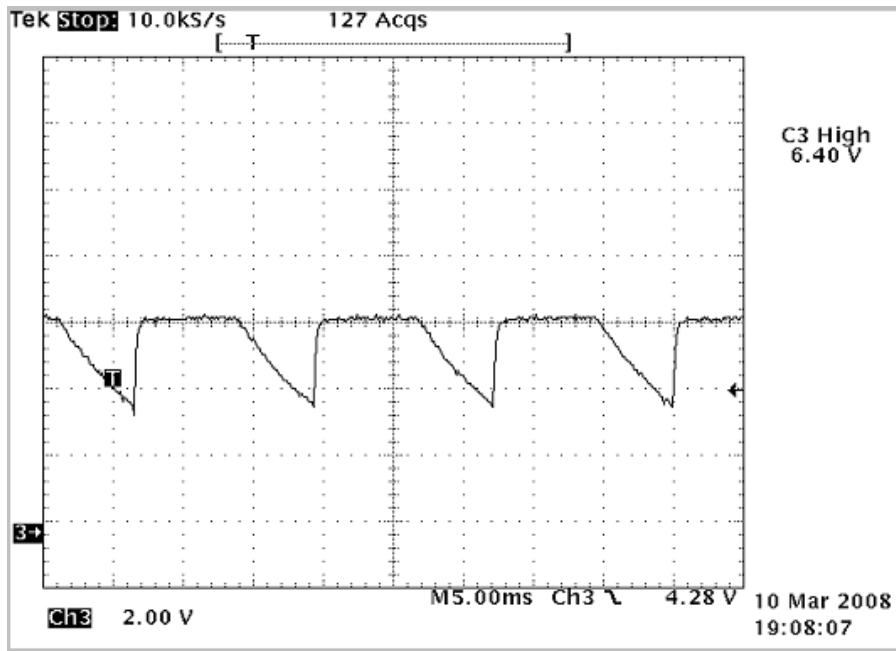


Figure 8. Pin 8,U30. There is USB link. Umbilical power is OFF. Battery is present, but it is OFF.

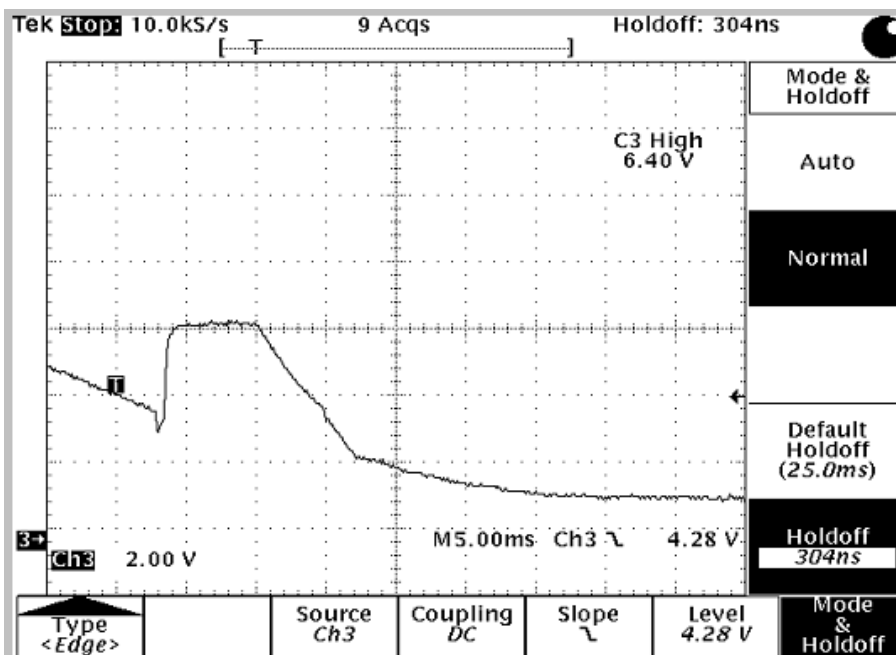


Figure 9. Pin 8,U30. Umbilical power ON -> OFF. Battery is present, but it is OFF

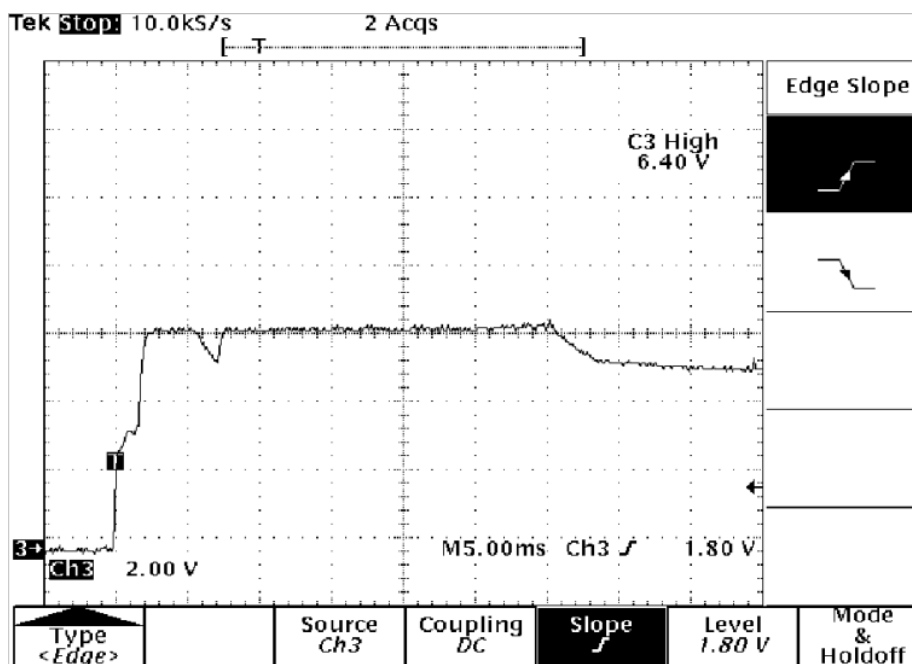


Figure 10. Pin 8,U30. Umbilical power OFF -> ON. Battery is present, but it is OFF

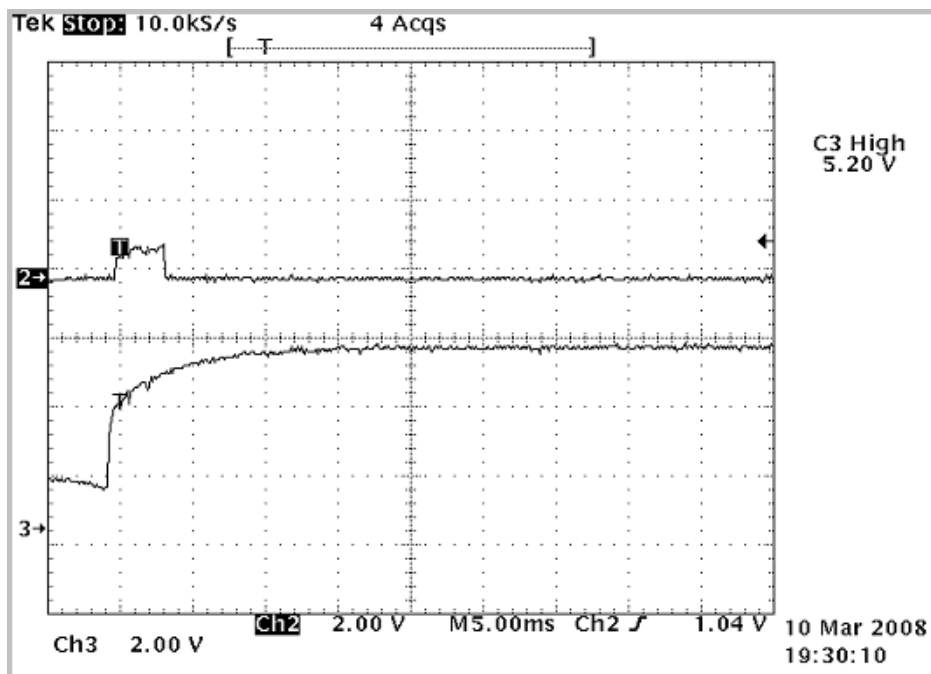
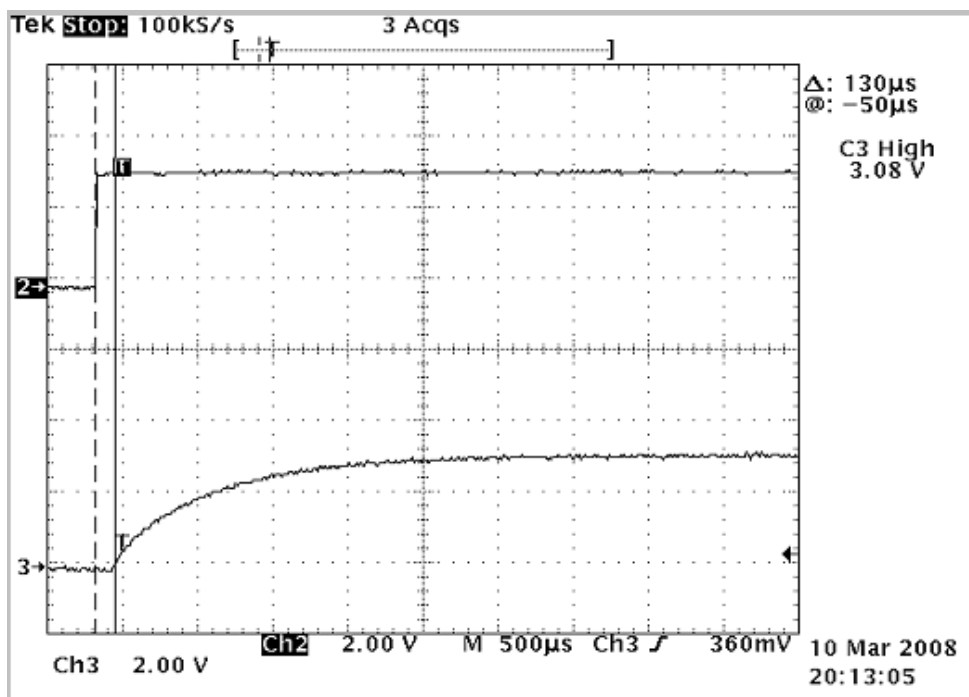
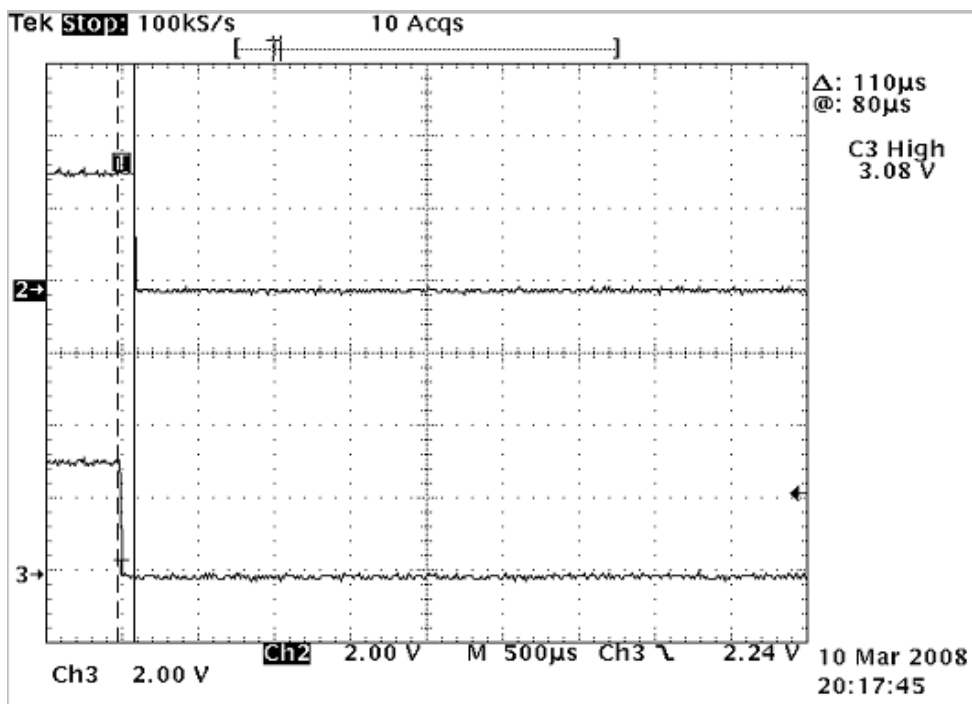


Figure 11. Channel 3: Pin 8,U30. Channel 2: Pin 4, U5. Umbilical power OFF -> ON.



**Figure 12. Channel 2: Pin 4,U6. Channel 3: Pin 4, M12. Umbilical power OFF -> ON.
Battery is present.**



**Figure 13. Channel 2: Pin 4,U6. Channel 3: Pin 4, M12. Umbilical power ON -> OFF.
Battery is present.**

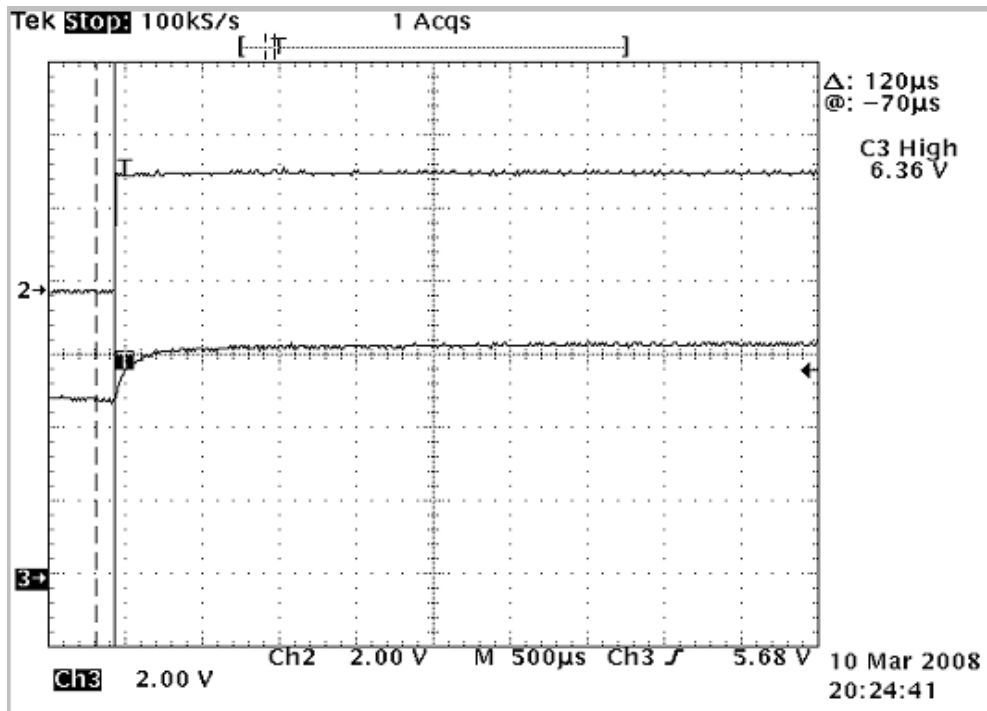


Figure 14. Channel 2: Pin 4,U6. Channel 3: Pin 8, U30. Umbilical power ON -> OFF. Battery is present.

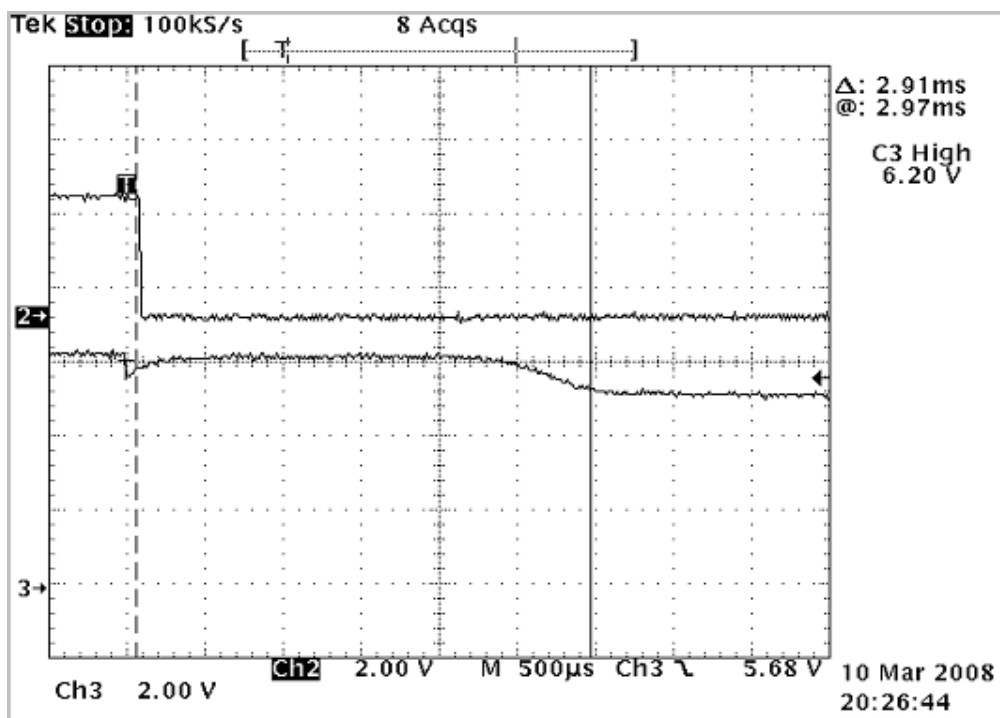


Figure 15. Channel 2: Pin 4,U6. Channel 3: Pin 8, U30. Umbilical power OFF -> ON. Battery is present.

5.2 Power Failures During Testing

When running from battery power, the umbilical power was connected, then possibly disconnected and reconnected. Somewhere along this process, an event occurred in the transitions that resulted in destruction of U30, the negative voltage regulator that provides a -5V rail that is subsequently regulated down to -3V3. The regulator is a MAX1044. This occurred on two out of twelve units tested

5.3 Waveforms on U30 under full load (worst case conditions): SOV, 2 injectors, LEDs, Scrubber stick, speaker etc.

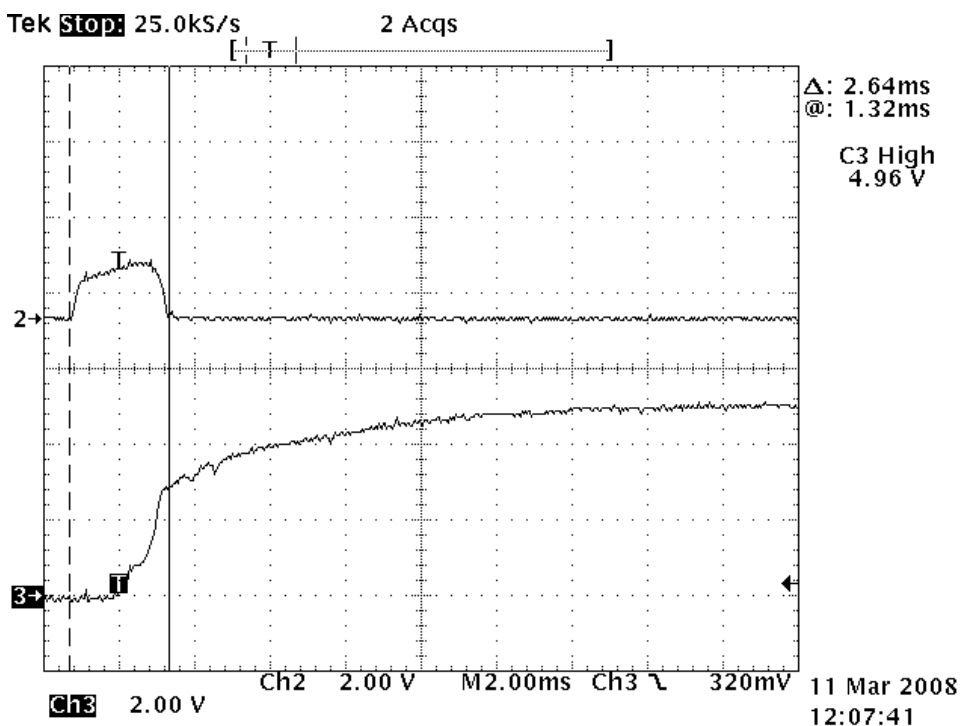


Figure 16. Channel 3: pin8, U30; Channel 2: pin4, M12. Umbilical Power OFF->ON. Battery is absent.

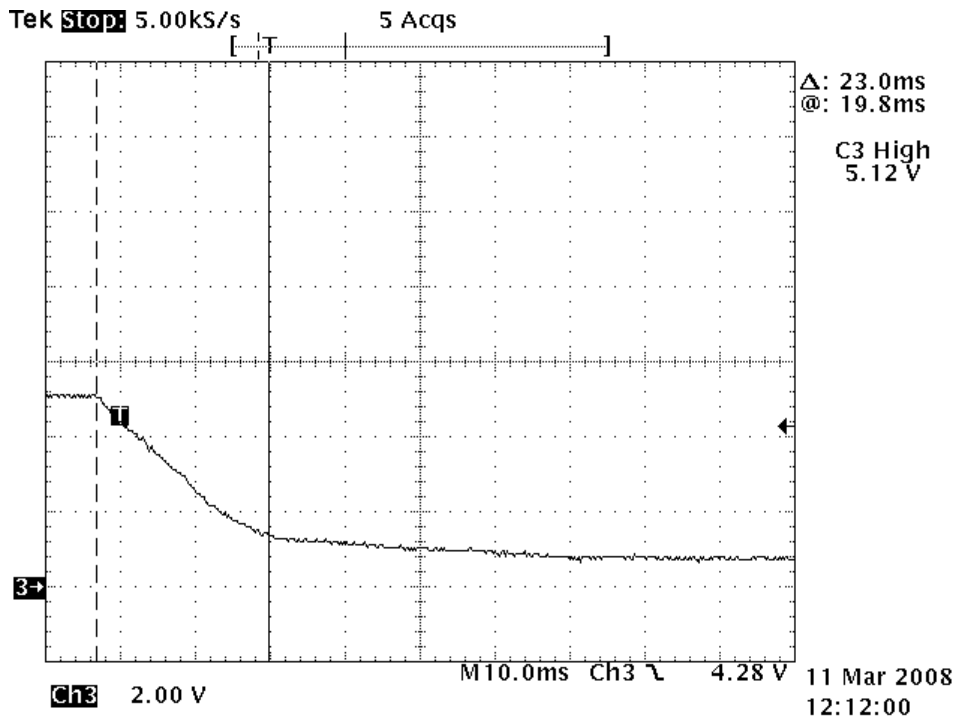


Figure 17. Pin8, U30; Umbilical Power ON->OFF. Battery is absent.

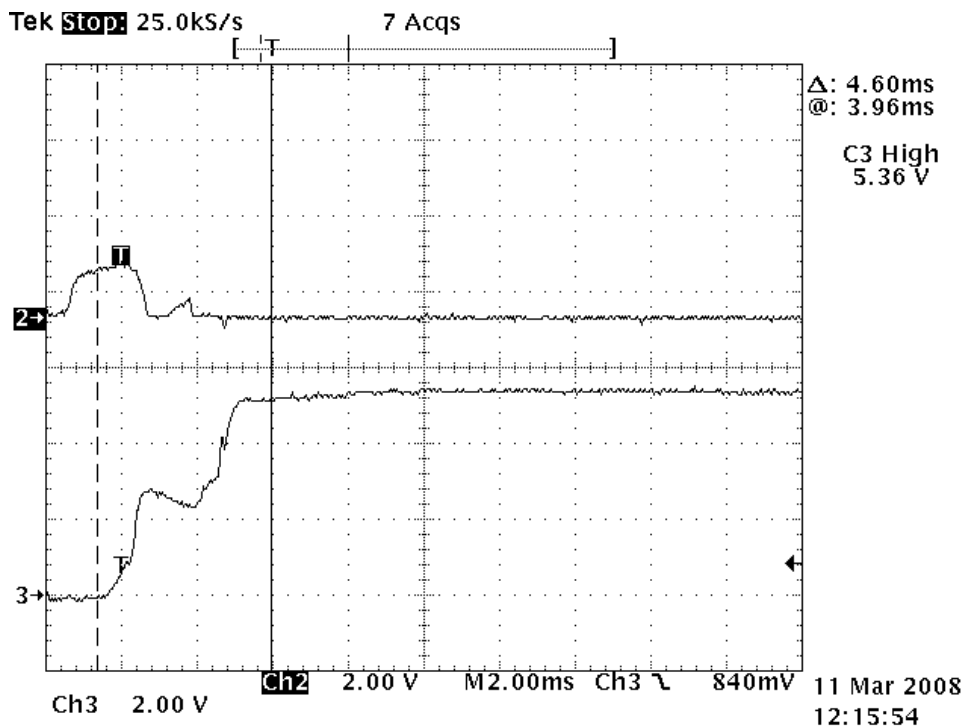


Figure 18. Channel 3: pin8, U30; Channel 2: pin4, M12. Umbilical Power OFF->ON. Battery is present.

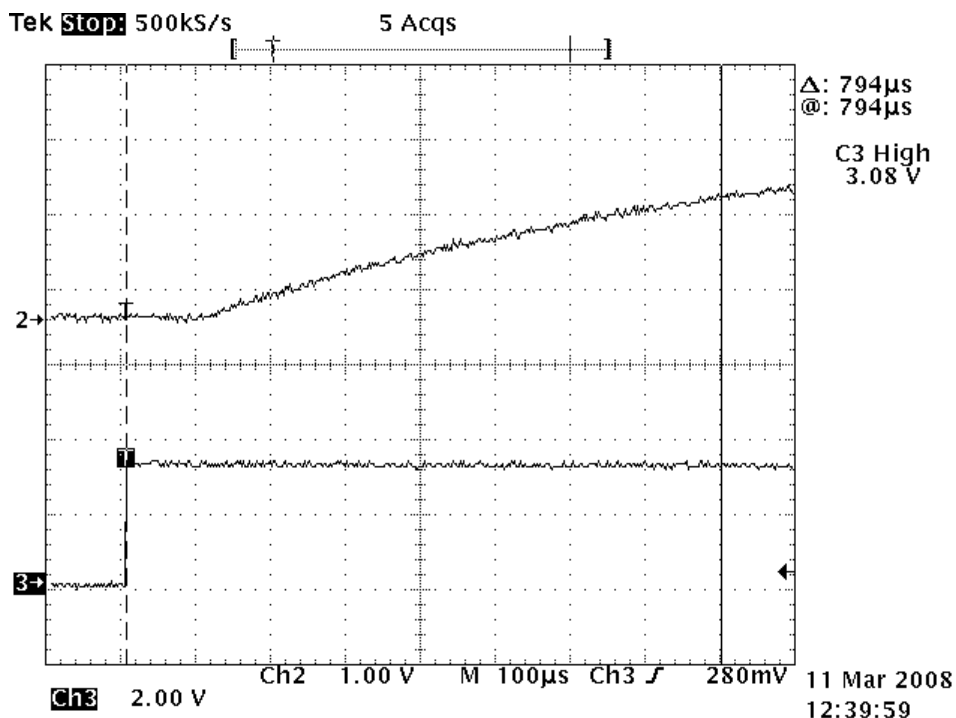


Figure 19. Channel 3: pin4, U6; Channel 2: pin4, M12. Umbilical Power ON->OFF. Battery is present.

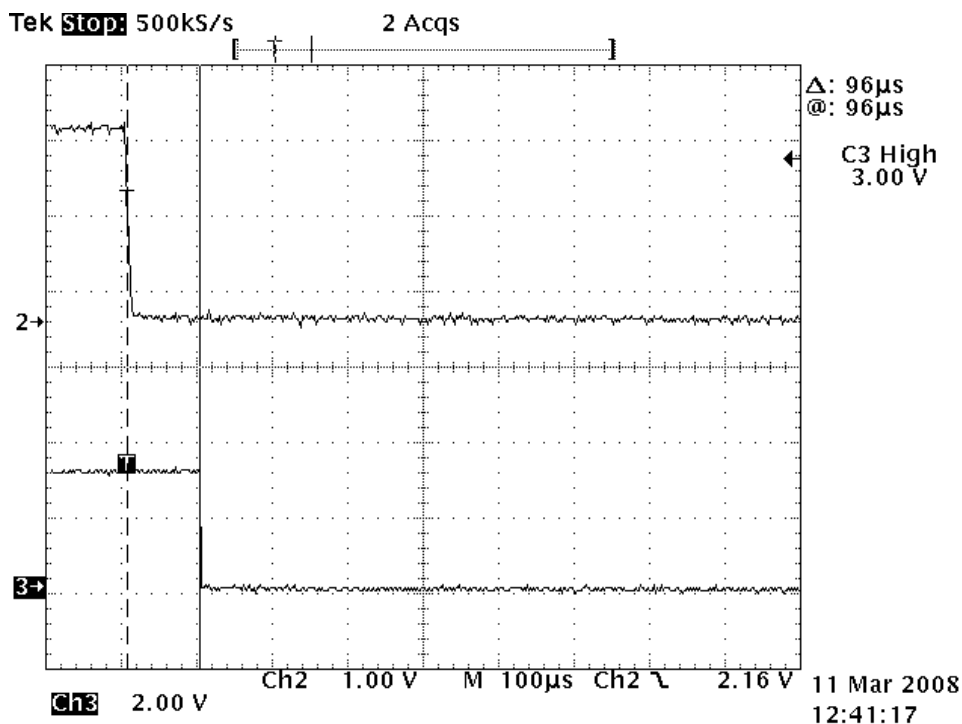


Figure 20. Channel 3: pin4, U6; Channel 2: pin4, M12. Umbilical Power OFF->ON. Battery is present.

5.4 Independent review of U30 reliability

An independent review was made, the review panel comprising the authors of this report: the Design Authority is Marat Evtukov.

U30 is a stable part from a reputable company (Maxim). The higher voltage rating makes it slightly preferable to the plug compatible part from Linear Technology, but Maxim is rated B- as a supplier by Deep Life due to long lead times and high minimum order quantities. Given the failure of this part, the Linear Technology part should be moved to the preferred source for this component, and Maxim as the second source.

The review of U30 did not have not find anything specific what may cause premature failure. It appears to operate within safe margins for both input and output.

The following issues were considered in detail, in addition to the general data sheet and circuit review, with comparison with the measured waveforms:

1. It is synchronised with a 62.5kHz source to minimise conversion noise in the ADCs that use the negative rail that U30 generates. There is no possibility of a current from load to source, as there is a FET isolating U30 from the clock source.
2. It may have sense to include simple RC filters on the input and on the output. Something like 100 Ohm and 10uF may work well.
3. There is a concern regarding the way over voltage protection switches are operating. It uses FDS4072N3 NMOS switches to pass power to microcontroller and FPGA. These switches have input voltage on their gates and drain and source at 3.3V. This transistor has a maximum V_{gs} 3.0V at 25C and 250uA channel current. With MUX voltage of about 5.8V it may not guaranty more than 2.8V instead of 3.3 and at very low current and at the room temperature. Generally it is not the ideal way to control high side switches but it does not explain any failure in U30.
4. Passing control signals through XOR gates may need further verification. However as soon as there is no input voltages more than 7V there appears to be no risk to damage U30 through that route.
5. There is no means to limit current between batteries and MUX output. There is a diode in the MUX power supply protecting from the reverse current but whole MUX will be powered from batteries until switches are reconfigured. It may pull the whole rail very low in worst case causing power failure in FPGA and MCU.
6. There is a general concern that the MCU and the FPGA must act very fast to prevent the loss of power, when umbilical power drops out. A diode scheme is preferred by the reviewers, but after consideration of the fail-safe backstop using the RTC, accept that the scheme is suitable for a safety system.
7. There are two converters of this type working in parallel and if the problem is always with only one of them then it is unlikely anything wrong with input voltage present in POWER_SUPPLIES net. Investigating problem in the lab may involve swapping loads and control between them to see would another converter also burned or not.
8. Converters are loaded with the same loads through another linear regulator and also they are tolerant to the continuous short circuit on their output. The reviewers cannot see how over-current drain on the circuitry load may overheat them.
9. The failure of U30 is probably be due to an assembly problem with particular boards, such as shorts to other nets, problems with particular components, e.g. ESD damage. Shorts may be via other boards if they happen through conductive mechanical elements.
10. The reviews checked plots in the previous sections and did not identify any suspicious behaviour.

6 BATTERY HOUSINGS

The battery housings twist the batteries when they are screwed onto their seats. This is highly undesirable.

Action: A change to the battery housings is required to restore the end cap, so the batteries are not twisted at all when the battery housing is fitted.

7 CONCLUSIONS

- ◆ The power scheme appears to achieve the design intent safely.
- ◆ There is no circuit design fault causing U30 to fail prematurely: it is likely due to a manufacturing fault. Further empirical testing is required.
- ◆ Several improvements were identified for the battery housing and battery switching scheme. An ECO is being raised to address these issues: see next Section.
- ◆ The reviewers accepted the present switching scheme works.

8 ENGINEER CHANGE ORDER REQUIREMENTS

An Engineering Change Order (ECO) is being raised to:

1. Replace power switching FETs with diodes to avoid need to have MCU or FPGA
2. Change MUX wiring and Base unit wiring, so Vbus pin connecting the two, uses only one pin: on the left side. The right hand side becomes the PFD data pin, which is respect to ground. Base unit is the only connection to the PFD, connecting to MCU only: the PFD is a monitor. The Base unit has to relay Diver Alert Switch and Helmet Open Switch data back to the MUX: it becomes part of the Base unit status frame.
3. Base unit should integrate data on loss one of the two power sources, and put that data into the comms frames it sends out to the MUX and the PFD.
4. The PFD should read the power records in a comms frame to give a voice message on losing a power source, repeated every minute. The message should be “Lost umbilical power. Abort dive.”, or “Lost battery power. Abort dive.”
5. Allow the Base to power the PFD from its battery power. To do this, put FET and op-amp in parallel with a protective diode in the Base to provide a source limited to 250mA from the Base Unit to the MUX power pin, so the MUX can maintain the PFD only. Add an extra diode to the MUX just in front of the connection to the Base that stops the Base from powering the MUX. Add a linear regulator to the PFD to reduce the voltage from the Base Unit to 3V3.
6. Change the battery housing to use an end cap, so batteries are not rotated when they are installed or when a technician needs to apply a complete power down.
7. Provide means to disconnect the batteries using a crimped connector, to completely power down the rebreather.

9 REFERENCES

1. RB Base Unit schematics