

VERIFICATION OF FAIL-SAFE OXYGEN DOSING IN DEEP LIFE'S OPEN REVOLUTION FAMILY OF REBREATHERS

DOCUMENT: DV_Safe_O2_dosing_080516.doc
[Filename]

ORIGINATOR: Dr. Bob Davidov, Dr. Alex Deas

DEPARTMENT: Verification

LAST UPDATED: 16th May 2008

REVISION: B1

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

Controlled
Document

Confidential Document
Unclassified if blank.

Revision History

Revision	Date	Description
A	18 th Jan 2006	Formal verification results, A1 after proof reading, published as SC_Orifice_Criticality_070118.pdf
B, B1	16 th May 2008	15 th May 2008: Addition of empirical test results, B1 on 16 th May 2008 with clarifications following review by Technip Norge AS.

Copyright 2007,2008 © Deep Life Ltd.

All information and data provided herein are for general information purposes only
and are subject to change without notice or obligation.

Table of Contents

1. PURPOSE AND SCOPE	3
2. ABBREVIATIONS	3
3. OXYGEN FLOW	4
4. FORMAL VERIFICATION AND FAULT SIMULATION	6
4.1. Profile: 48m_deco (38 min at 48msw plus deco)	6
4.2. Profile: 91_180 Bounce dive to 91msw	8
4.3. Profile: AD_1901 Saturation Dive from 350m	11
4.4. Conclusions from Formal Modelling	16
5. PARAMETERS AFFECTING FAULT CRITICALITY	16
5.1. Definition of a fault condition	16
5.2. Probability of the O2 injector fault being a critical fault	16
6. CONTROL TO MITIGATE FAULT CRITICALITY	17
6.1. Example of a Safe Orifice Control Algorithm	17
6.2. Example of improvement using orifice limiting control	18
7. EMPIRICAL TESTS	21
7.1. Results of unmanned tests, extreme profile example	22
7.2. Results of manned test	23
8. CONCLUSIONS	23
CREDITS	24

1. PURPOSE AND SCOPE

The purpose of this document is to report a study into the criticality of a variable orifice gas injector failure. Such a failure may be due to failure of the power or drive electronics while the injector is in a position where the amount of oxygen injected differs from the mean metabolic rate, such that the PPO₂ would go outside the range 0.2 to 1.6 within 30 minutes of the fault occurring.

This study also has relevance to mCCRs, where there is a fixed orifice or a variable orifice set to the mean metabolic rate, and the user then adds oxygen manually.

Dives from 40msw to 600msw are considered, using a variable orifice, which when full open is between 300µm and 350µm.

Formal modeling methods are used to determine the risk given a set of events.

Following formal verification, the safety of the variable orifice valve with position limiting algorithm, was confirmed in both unmanned and manned tests by causing a sudden and total loss of all power at critical stages of the dive, using worst case gas mixtures.

The scope of this document is a safety analysis and design verification report within the safety case for the Deep Life O.R. rebreather design, in accord with Deep Life Quality Procedure QP-20.

2. ABBREVIATIONS

ALARP: As Low As Reasonably Practicable, meaning the risk is as low as practicable applying good practice. In Norway and other countries with Objective Safety Responsibility is applied, then ALARP generally is relative to best practice.

PPO₂: Partial Pressure of Oxygen, in ATM unless otherwise stated (1 ATM = 1.013 bar).

<Remainder of page intentionally blank>

3. OXYGEN FLOW

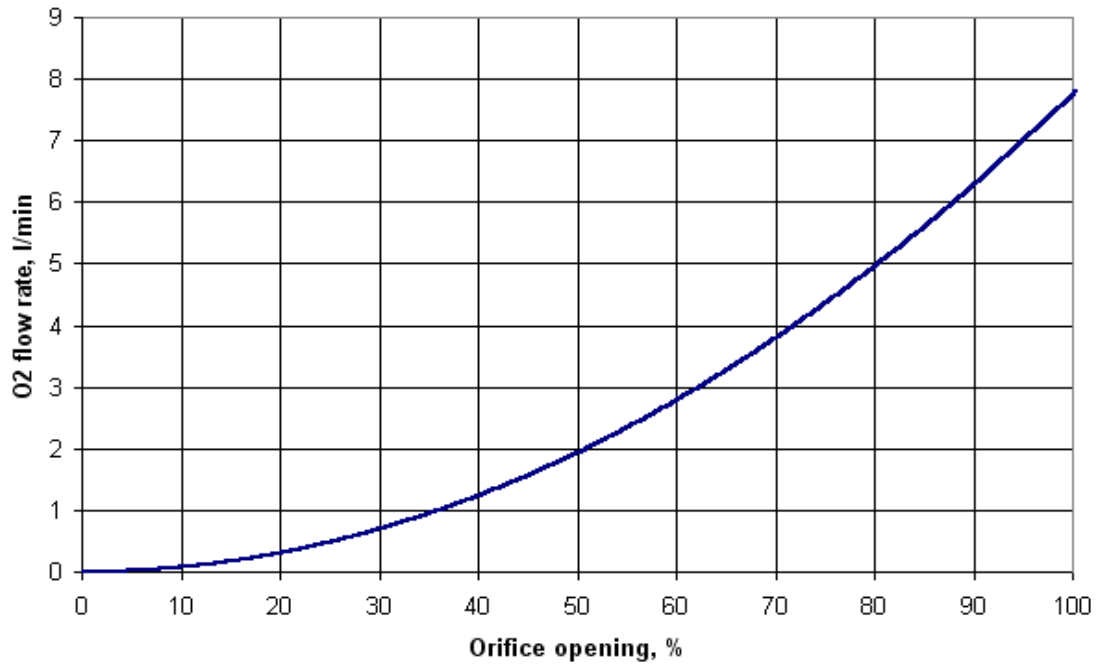


Figure 3-1. Oxygen flow through a 0 to 300µm variable orifice. Non compensated valve: i.e. intermediate pressure does not vary with ambient pressure. Intermediate pressure is 10 bar. Relation of flow to orifice opening is independent of depth where the ambient water pressure is less than half the intermediate pressure.

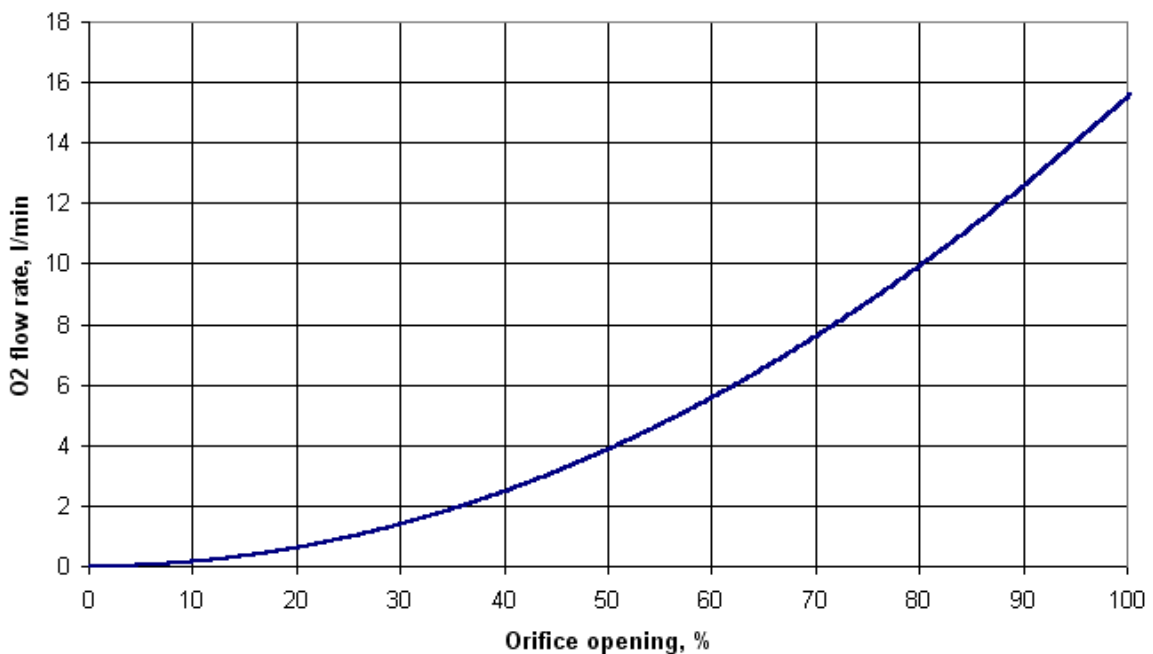


Figure 3-2. Oxygen flow through a 0 to 300µm orifice. Non-compensated valve. Intermediate pressure is 20 bar.

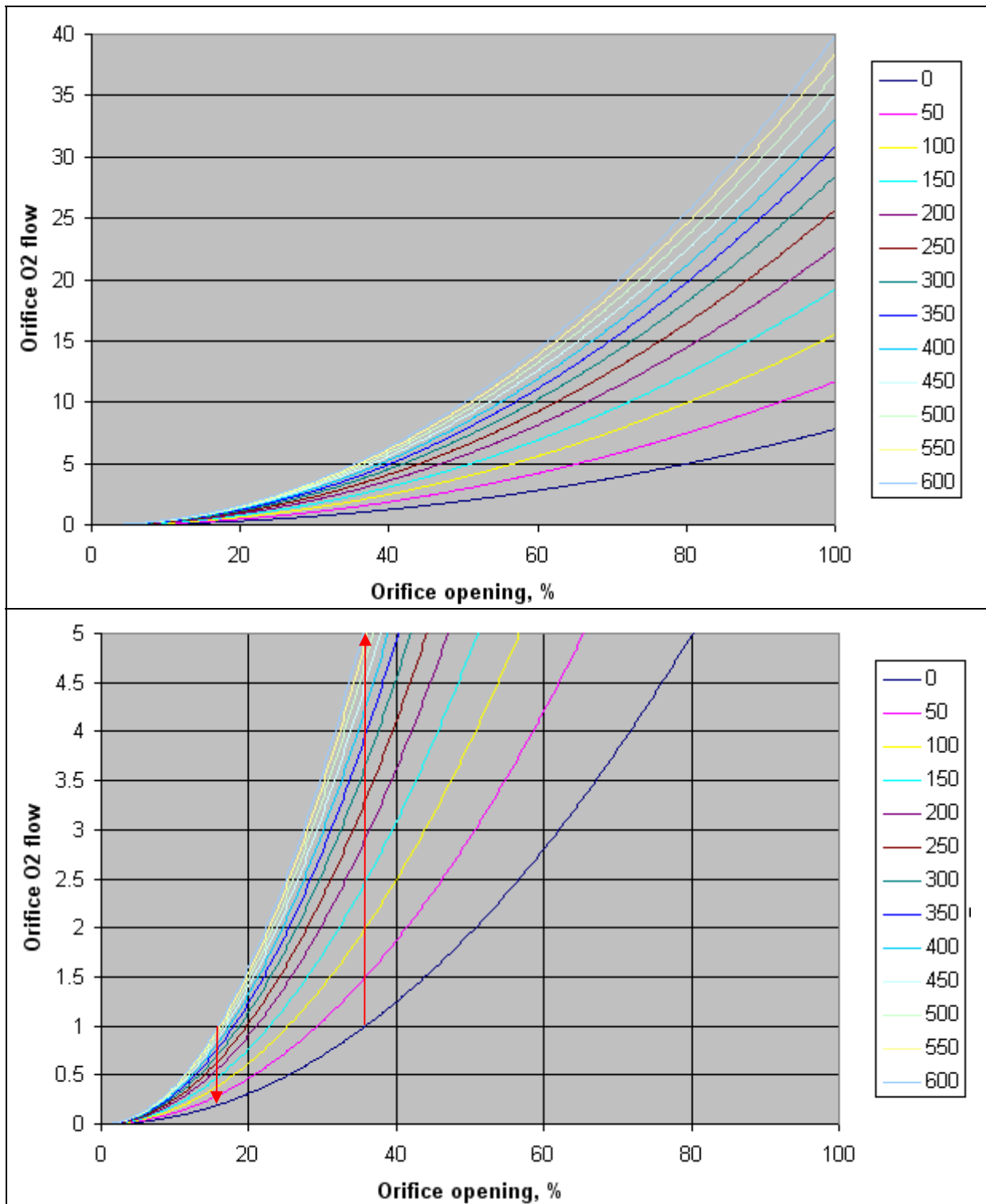


Figure 3-3. Orifice flow through a 0 to 300 μ m orifice of compensated gas injector: i.e. the first stage maintains a constant intermediate pressure with respect to the ambient pressure. Intermediate pressure is 10 bar above ambient. The same opening of 1 l/min flow at surface provides 5 l/min flow at 600m depth, and an opening of 1 l/min flow at 600m provides 0.2 l/min flow at surface. When orifice flow is subsonic, the orifice opening is larger to maintain a given oxygen flow. Note the two graphs are the same, but the lower graph is a zoom for the lower flow rates.

4. FORMAL VERIFICATION AND FAULT SIMULATION

The method used for formal verification was that of Monte Carlo Fault Simulation, from which are taken the following Example Dive Profiles. The formal model is the Deep Life Rebreather Environment Model version 3.1: this is published on www.deeplife.co.uk/or_model.php

4.1. Profile: 48m_deco (38 min at 48msw plus deco)

Initial state:

- Diluent gas: 5% O₂, 95%He with CCR using pure O₂
- Metabolic rate is 1 l/min
- PPO₂ set is 0.7 ATA
- Breathing loop volume is 6 litres
- First stage valve is not compensated
- Intermediate pressure is 10 bar
- Maximum orifice size is 300 μ m: it is adjusted to match the actual O₂ metabolised.
- Descent rate is 8 m/min
- Ascent rate is 0.9 m/min

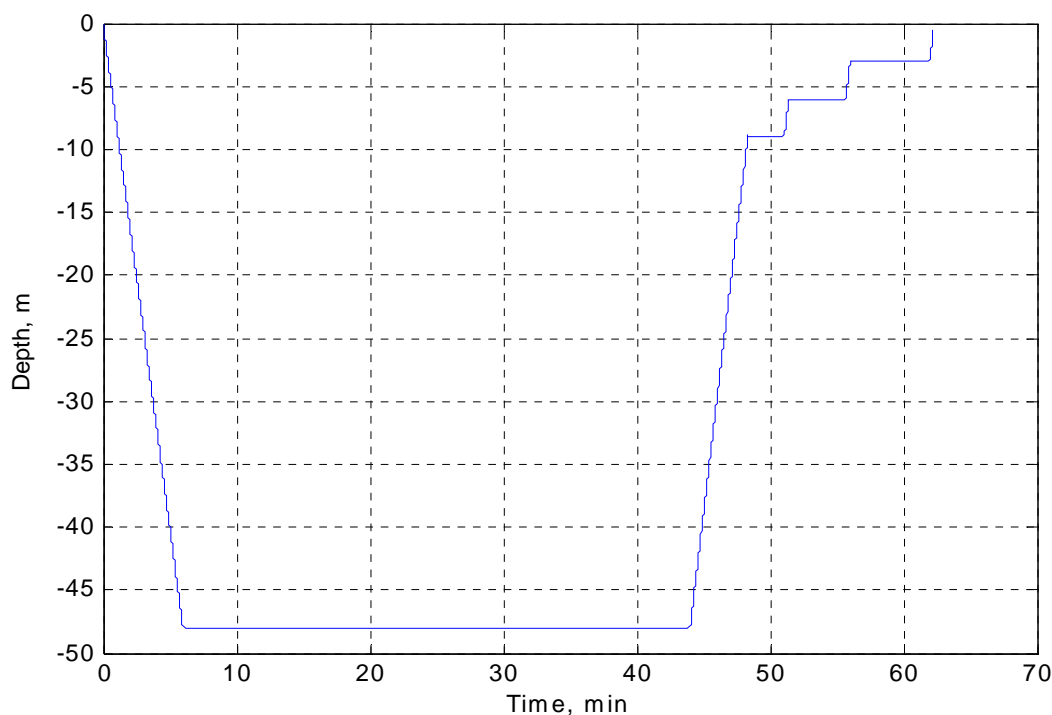


Figure 4-4. Depth profile.

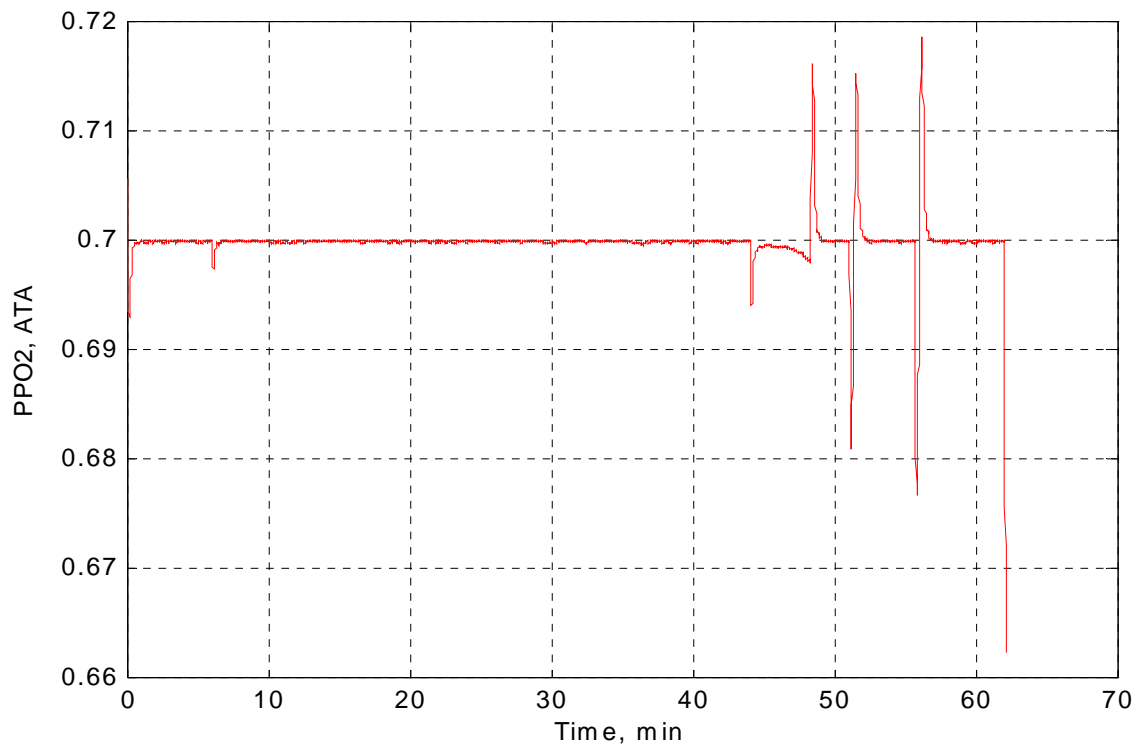


Figure 4-5. PPO2 in the breathing loop.

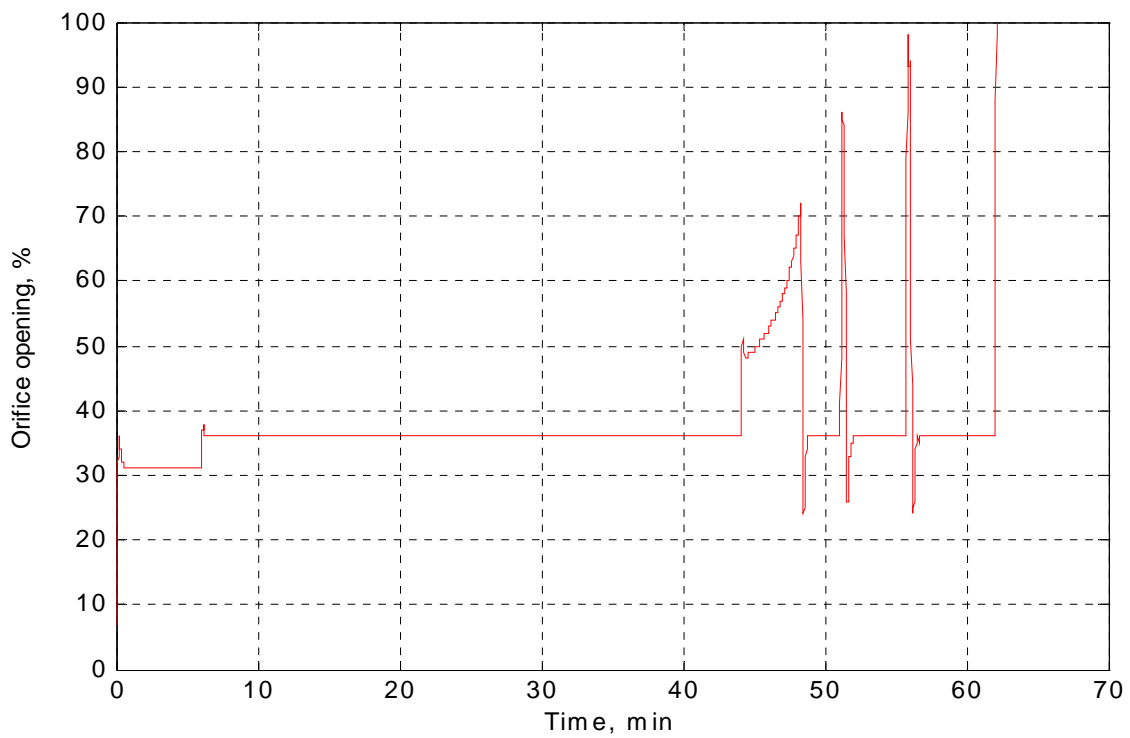


Figure 4-6. Orifice opening.

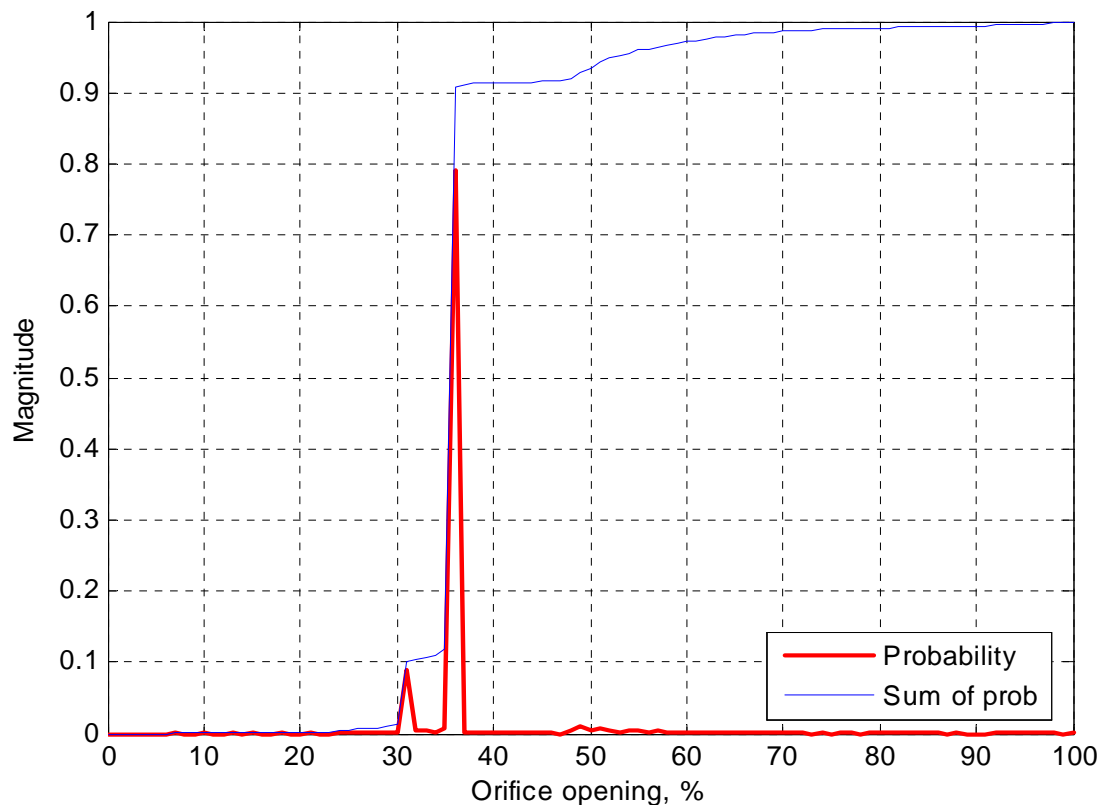


Figure 4-7. Orifice size probability.

4.2 Profile: 91_180 Bounce dive to 91msw

Initial state:

- Diluent gas: 5% O₂, 95%He with CCR using pure O₂
- Metabolic rate is 1 l/min
- PPO₂ set is 0.7 ATA
- Breathing loop volume is 6 litres
- First stage valve is not compensated
- Intermediate pressure is 20 bar
- Maximum orifice size is 300 μ m: it is adjusted to match the actual O₂ metabolised
- Descent/Ascent rate is according to the depth profile

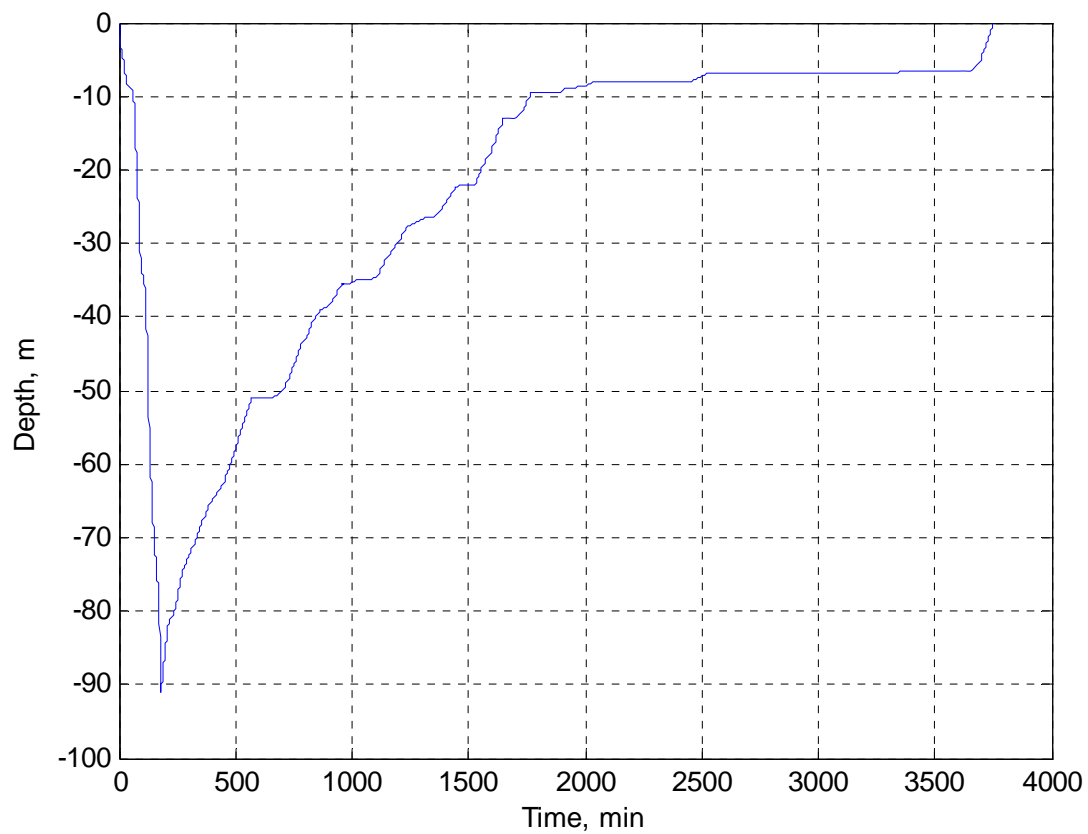


Figure 4-8. Depth profile.

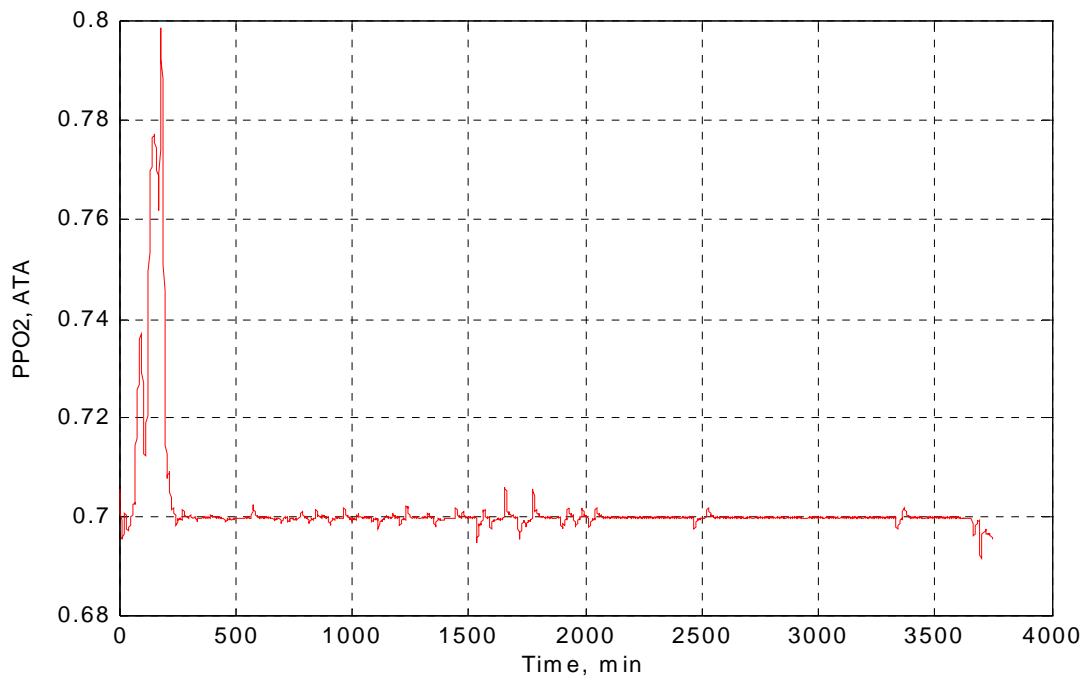


Figure 4-9. PPO2 in the breathing loop.

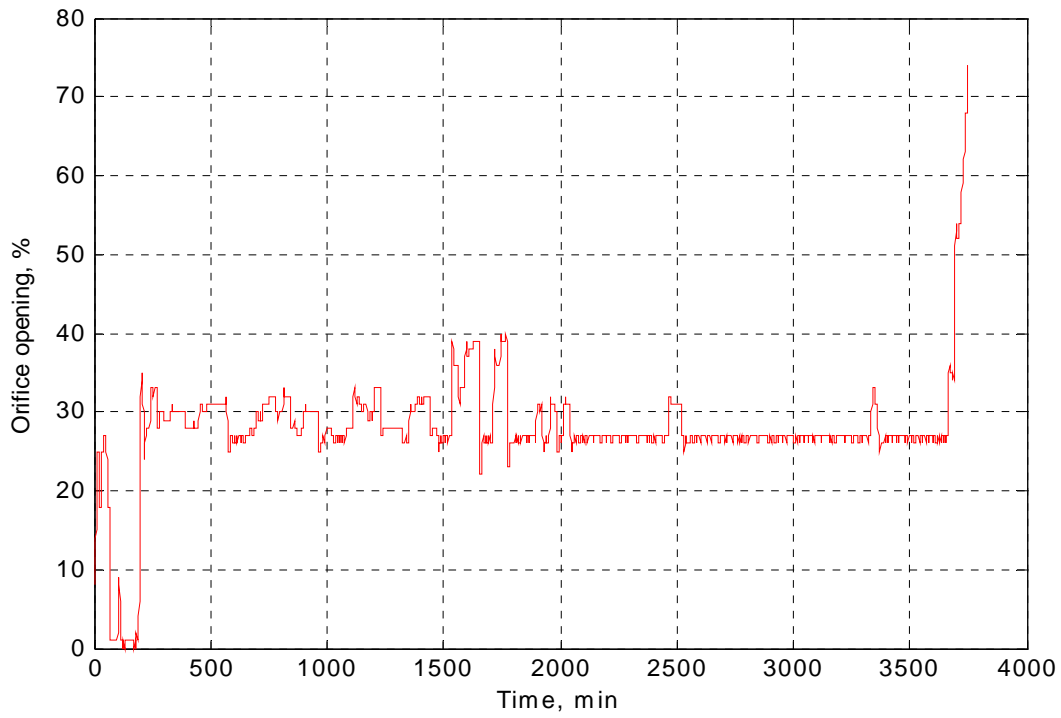


Figure 4-10. Orifice opening.

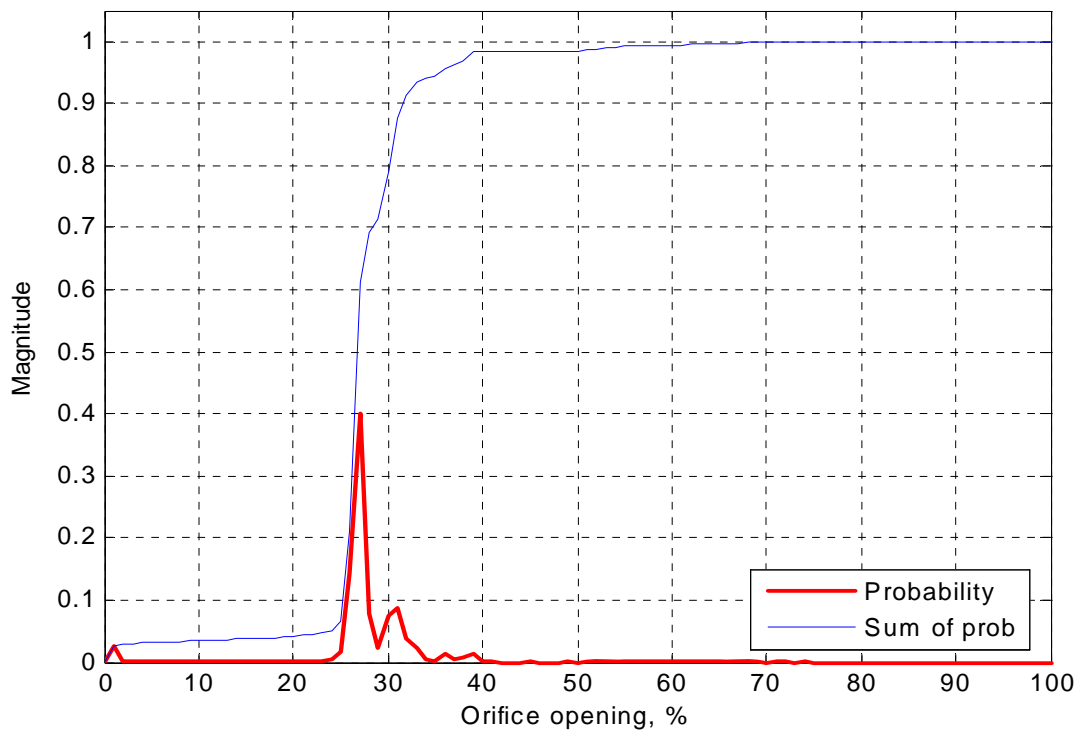


Figure 4-11. Orifice size probability.

4.3 Profile: AD_1901 Saturation Dive from 350m

Initial state:

- Make up gas: 4.44% O₂, remainder is helium, operating as SCR as >23% O₂ not allowed in bell.
- Metabolic rate range varies according to a profile from 0.5l/min to 2.0l/min of O₂.
- PPO₂ set is 0.7 ATA
- PPO₂ no fault range is 0.2..1.6 ATA
- Breathing loop volume is 12 litres
- First stage valve is compensated
- Intermediate pressure is 10 bar
- Maximum orifice size is 350µm: it is adjusted to match the actual O₂ metabolised.
- Orifice control type: analogue
- Initial depth is 350msw, with excursions of 20msw each way.
- Initial O₂ in the breathing loop is $0.7 \cdot 12 / (36 \cdot 12 - 0.7 \cdot 12) = 1.983\%$
- Fault criteria: PPO₂ in breathing loop gets limits of 0.2 or 1.6 ATA in 30 min after the injector stop. The injector flow rate over the metabolic rate is low than the 0.4 l/min and more than the 2.1 l/min. Max Asc/Dec rate to the depth of return of 350 m after the fault is 10 m/min.

Table 1. Profile data.

Time,min	0	30	40	50	60	70	80	90	100	110	120	130
Depth, m	350	350	370	370	370	370	330	330	330	330	350	350
Met.rate l/min	0.9	0.9	0.9	0.9..2	2..0.9	0.9	0.9	0.9..0.5	0.9..0.5	0.9	0.9	0.9
Des/Asc rate, +/- m/min	0	0..2	2..0	0	0	0..-4	-4..0	0	0	0..2	0..2	0

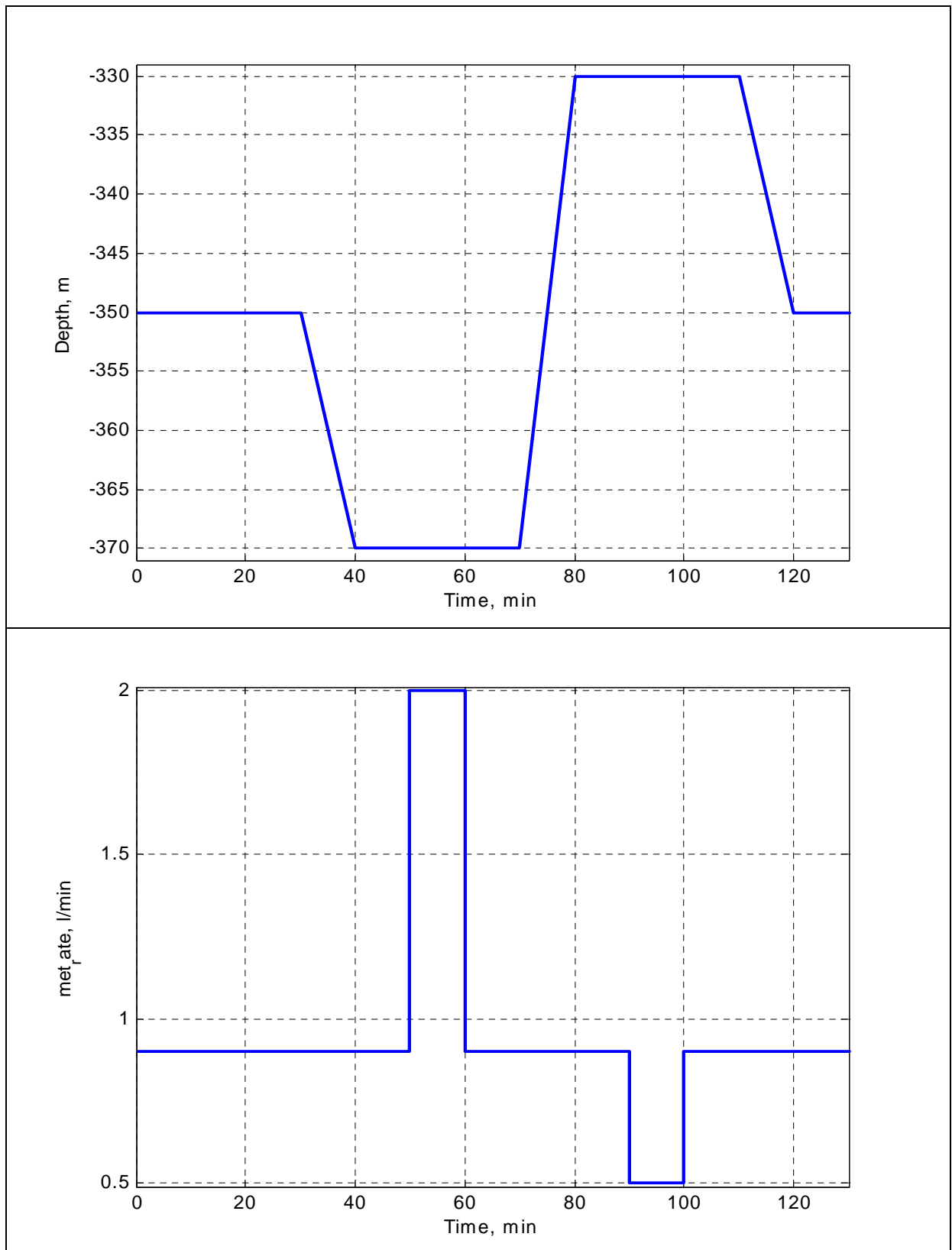


Figure 4-12. Dive profile and metabolic rate.

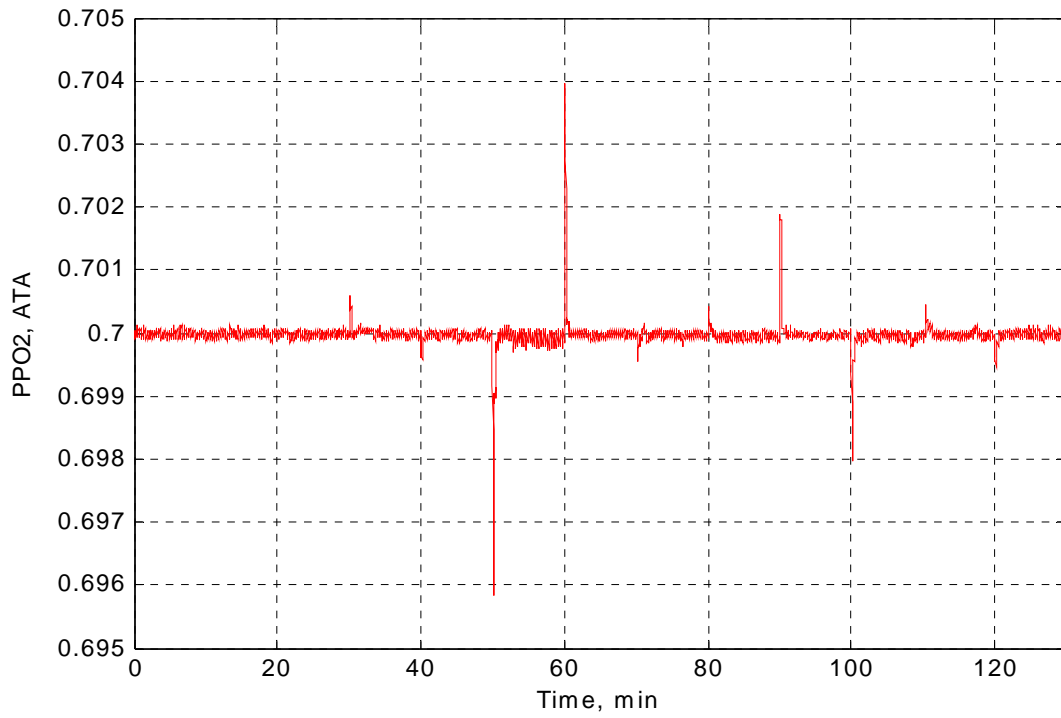


Figure 4-13. PPO2 in the breathing loop.

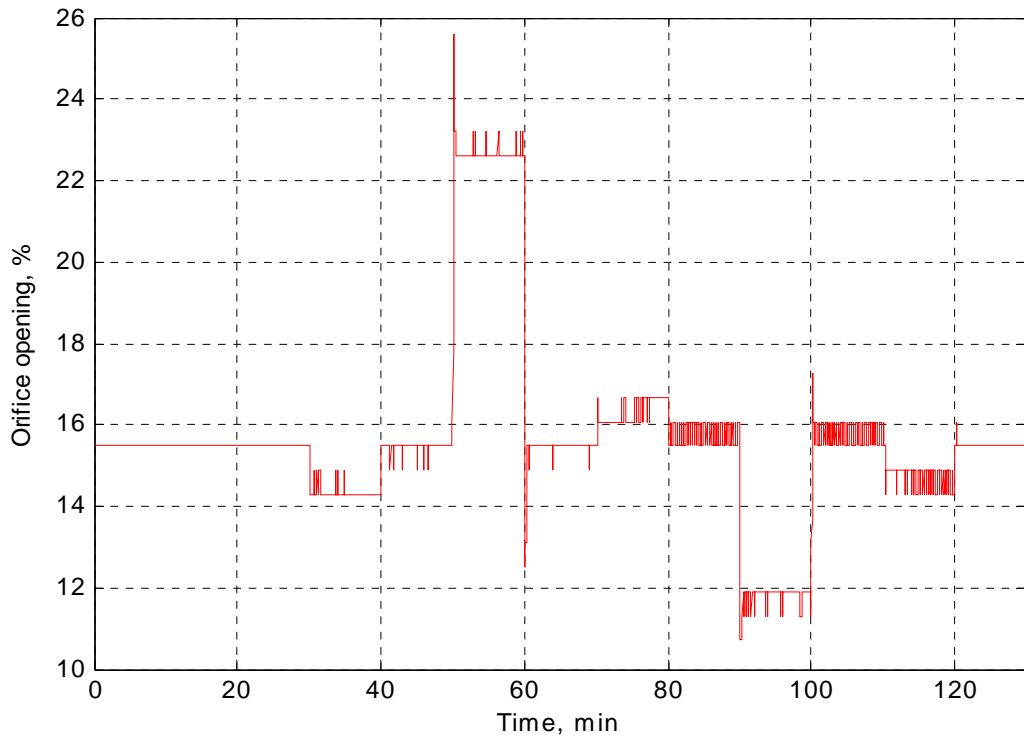


Figure 4-14. Orifice opening.

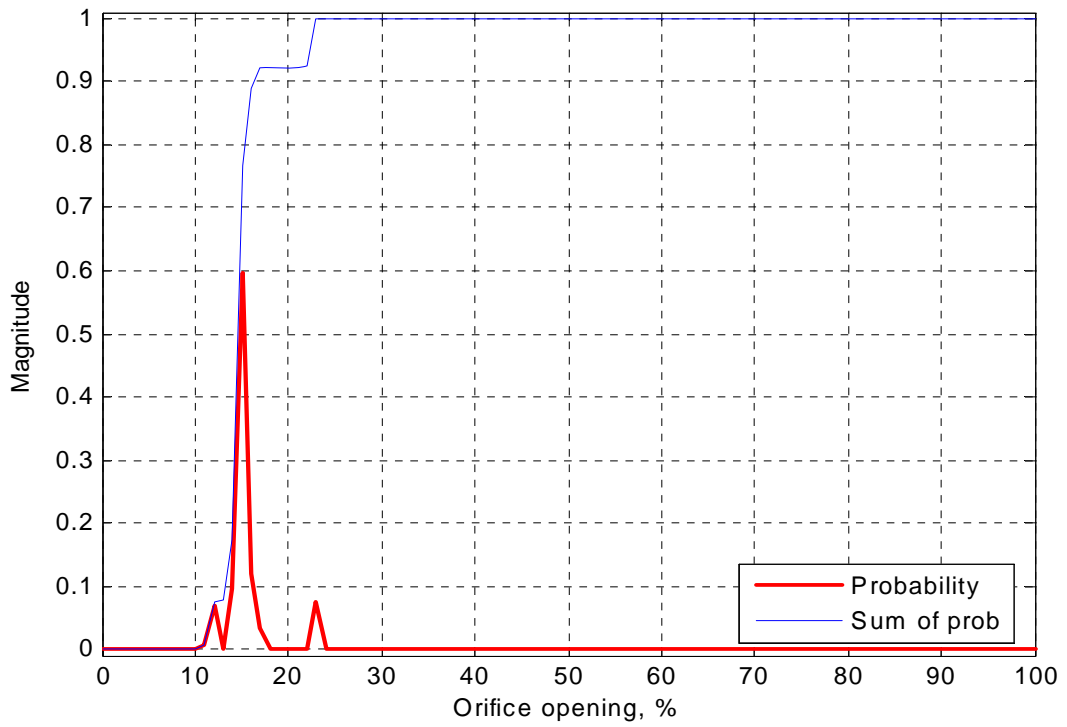


Figure 4-15. Orifice opening probability.

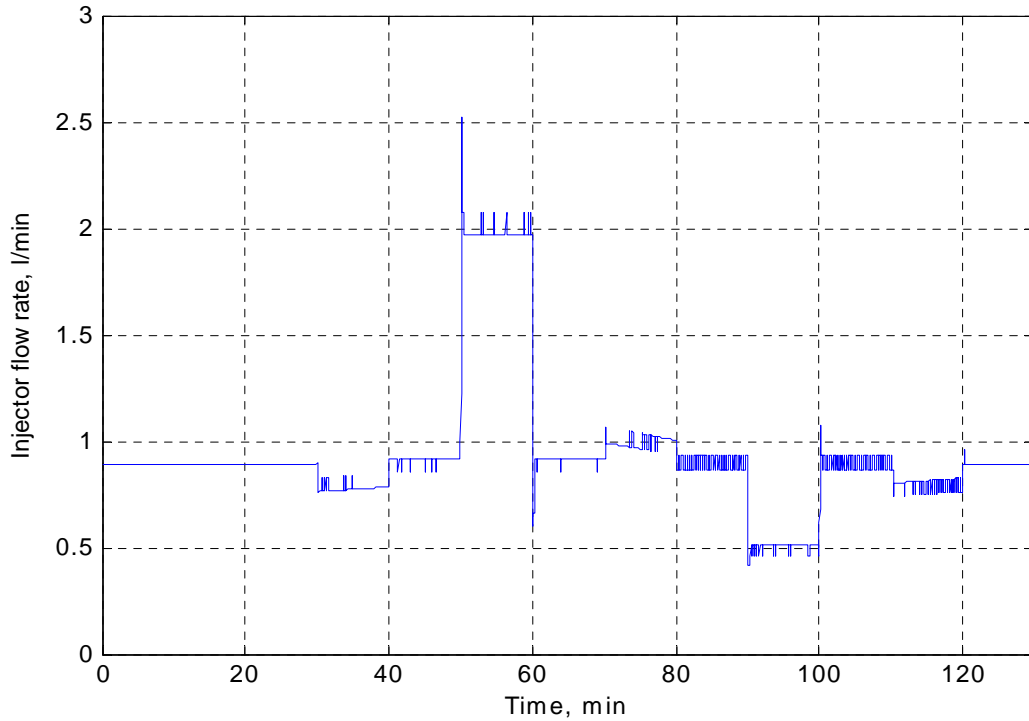


Figure 4-16. Orifice flow.

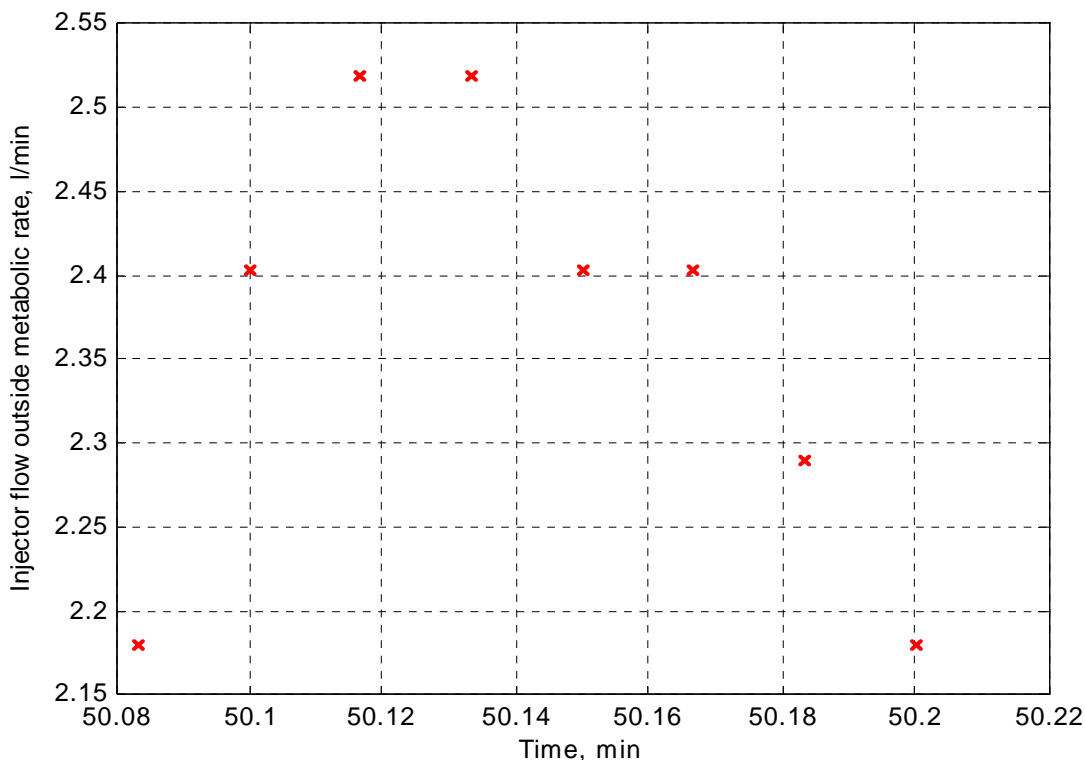


Figure 4-17. Events where gas injector flow exceeds metabolic demand. There are 8 points at [2.1797 2.4031 2.5189 2.5189 2.4031 2.4031 2.29 2.1797] at run times of [3005 3006 3007 3008 3009 3010 3011 3012]/60 min. There is event where the injector flow is less than 0.4 l/min metabolic rate.

The PPO2 in the breathing loop at run times of [3005 3006 3007 3008 3009 3010 3011 3012]/60 min are [0.69602 0.69598 0.69584 0.69628 0.6965 0.69719 0.69745 0.69807] ATA.

The orifice size at those run times is [78.571 82.5 84.464 84.464 82.5 82.5 80.536 78.571] um

The depth at hose run times is 370msw in each case.

The depth of the dive bell is 350 m. The flow through the stop injector orifice at 350 m is [2.117 2.335 2.447 2.447 2.335 2.335 2.225 2.117].

The ascend rate from 370m to 350m is 10 m/min, so it takes 2min to return from the excursion to the bell depth. The max time to the bell is 30 min. It means that the criticality condition is the orifice flow rate at 350 m minus 2.1l/min, i.e. [0.0797 0.3031 0.4189 0.4189 0.3031 0.3031 0.1900 0.0797] l/min.

During ascent O2 from the breathing loop as well as diluent, is lost from the breathing loop via the OPV. The PPO2 is decreased by approximately 0.19 ATA.

The volume of gas going into the breathing loop through the failed injector is (max_PPO2 – stop_injector_PPO2 + ascent_PPO2)*Breathing_loop_vol. The volume of O2 in the loop at standard pressure and temperature is (1.6 – 0.7 + 0.19)*12 = 13.08 litres. The time to inject that volume after the injector fails is [164.714 43.313 31.344 31.331 43.293 43.265 69.003 164.406] min. These times all exceed the time needed to return to the bell, of 30mins, so none of these failures are critical.

4.4 Conclusions from Formal Modelling

1. Example profiles are used here for illustrative purposes. Full conclusions should be based on the Monte Carlo analysis.
2. For the profile of AD_1901 and initial parameters, the probability of a stuck at injector fault being a critical fault is zero.
3. For surface dives, the probability of a stuck at injector fault being a critical fault is non-zero and can be significant. Action is required to reduce that risk to near zero.
4. Risks are higher the nearer to the surface, and higher the larger the variation in O2 demand.

5. PARAMETERS AFFECTING FAULT CRITICALITY

5.1. Definition of a fault condition

A critical fault condition has been defined as the diver having the PPO2 outside the range 0.2 to 1.6 before the diver can properly abort the dive. A fixed 30 minute interval has been allowed for the dive abort.

The justification for this 30 minute limit is:

- If the loop volume is 12 litres and the PPO2 set point is 0.7 (standard saturation diving practice and common SCUBA practice), then the PPO2 can vary safely by $-0.5/+0.9$. In the event the PPO2 set point is 1.3, a common SCUBA bottom PPO2 set point, the PPO2 can vary safely by $-1.1/+0.3$.
- In the worst case, of falling PPO2, then a change of 0.5 in PPO2 in 30mins is 0.2l of O2 per min of error.
- In the positive case, of rising PPO2 then the change of 0.9 in PPO2 in 30mins is 0.36l/min. For the SCUBA case with the PPO2 set point of 1.3, the time available before the fault becomes critical is reduced by a factor of 3, from 30mins to 10mins.
- If a fault condition occurs where the orifice is stuck, the PPO2 monitoring shows this and the diver has 30mins to return to the bell or to the surface. The commercial diver is restricted in umbilical length from 45m to 100m depending on the country involved and the conditions. After consideration of the time the diver may need to traverse this umbilical under poor conditions, an acceptable dive abort (bail-out) time of 30 minutes was specified as a requirement for this equipment.

Given the wide variation in PPO2 set points, the 0.7 PPO2 point is used in this study. In this case, if the rate of O2 injection is less than the metabolic rate by 0.2, or exceeds the metabolic rate by 0.36l/m then that is a critical failure.

5.2 Probability of the O2 injector fault being a critical fault

The probability of an injector fault becoming a critical failure depends on many factors, including:

- O2 fraction in diluent gas. The higher the fraction, the higher the criticality probability of the fault, except near the surface where the converse is strongly the case.
- Descent rate when the O2 fraction in diluent gas is more than zero. The higher descent rate, the higher the criticality probability.
- Ratio between the ascent/descent time and the constant depth time. When the ratio is low then the criticality probability is low, and the converse is also true.

- Range and profile of the set PPO2 as function of depth. The higher range increases the criticality probability.
- Type of first stage valve: a valve without depth compensation has a lower fault probability than a valve with depth compensation.
- Depth range. For example, ascending from 230msw to 200msw with the initial PPO2 set point of 1 ATA decreases the PPO2 by just 13%: $(3/23)*100\%$. An ascent from 30msw to the surface decreases PPO2 by 75%: $(3/4)*100\%$. This is in addition to reductions in PPO2 from metabolism.
- Metabolic rate range. The higher the variation in metabolic rate, the higher the fault probability.
- Time required to abort the dive after the injector fails. It is proportional to the distance between the point of injector failure and the bell, or the time to surface depending on whether it is a saturation dive or a surface dive.
- Possible min/max value of PPO2 in the breathing loop. This study has taken the non-critical range as being a PPO2 from 0.2 to 1.6 ATA, but some individuals may tolerate higher PPO2s for longer than others.
- Value of PPO2 in the breathing loop when the injector fails.
- Quality of the control algorithm. Control algorithms can reduce the criticality probability considerably by limiting the orifice excursion and allowing the PPO2 to vary over a wider, but safe, for very short periods of the dive. An example of such an algorithm is given in the section below.

6. CONTROL TO MITIGATE FAULT CRITICALITY

There are several methods that are apparent that reduce the criticality of an injector fault. These include:

1. In the case of a mCCR, such as when a variable orifice eCCR fails, the unit should operate as a pure oxygen rebreather when closer than 6m to the surface.
2. The eCCR or eSCR should limit the orifice excursion so the risk of a failure occurring when the orifice is in an abnormal state can be reduced, generally to zero. This sounds as if it would cause wild fluctuations in PPO2, but formal modelling of such algorithms shows this need not be the case.

6.1. Example of a Safe Orifice Control Algorithm

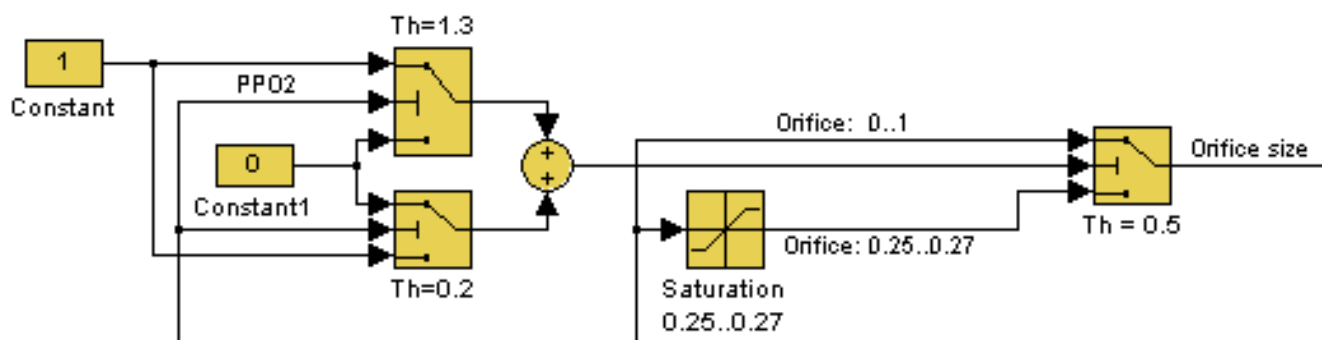


Figure 6-18. Part of the control structure for metabolic rate 1 l/min. The range of the 0.25..0.27 saturation must be calculated automatically according to the possible variation of

metabolic rate, taking into account the orifice flow of the type of first stage valve that is used, intermediate pressure and orifice opening.

6.2. Example of improvement using orifice limiting control

Initial state:

- Diluent gas: 5% O₂, 95%He
- Metabolic rate is 1 l/min
- PPO₂ set is 0.7 ATA
- Breathing loop volume is 6 litres
- First stage valve is not compensated
- Intermediate pressure is 20 bar
- Orifice size is 300µm
- Profile: prof 91_180 – a bounce dive to 91msw
- Descent/Ascent rate is according to the depth profile
- Metabolic rate control range: from 25% to 27% of orifice range or from 0.973 to 1.135 l/min O₂ rate

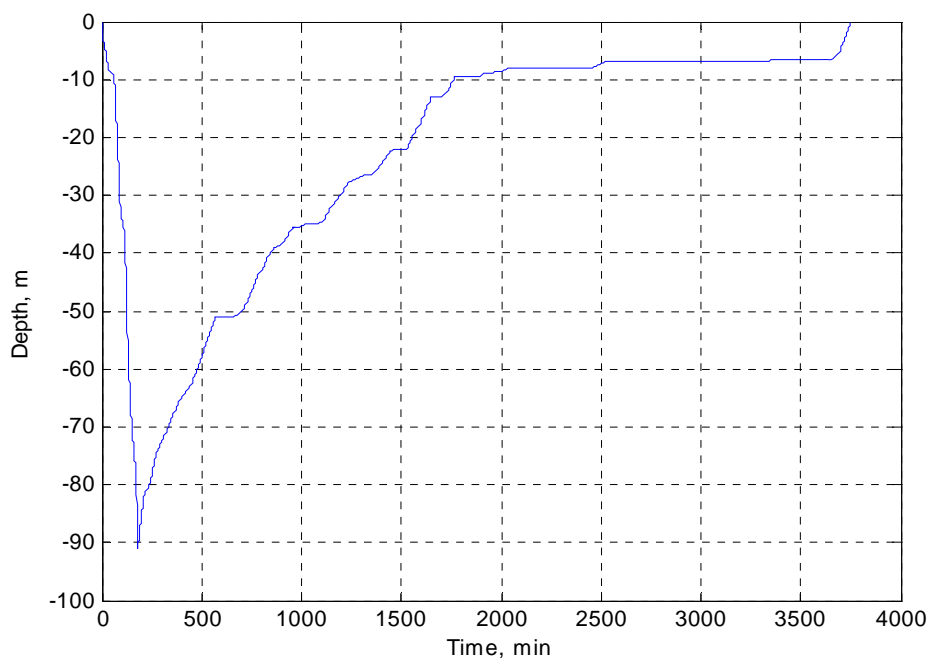


Figure 6-19. Depth profile.

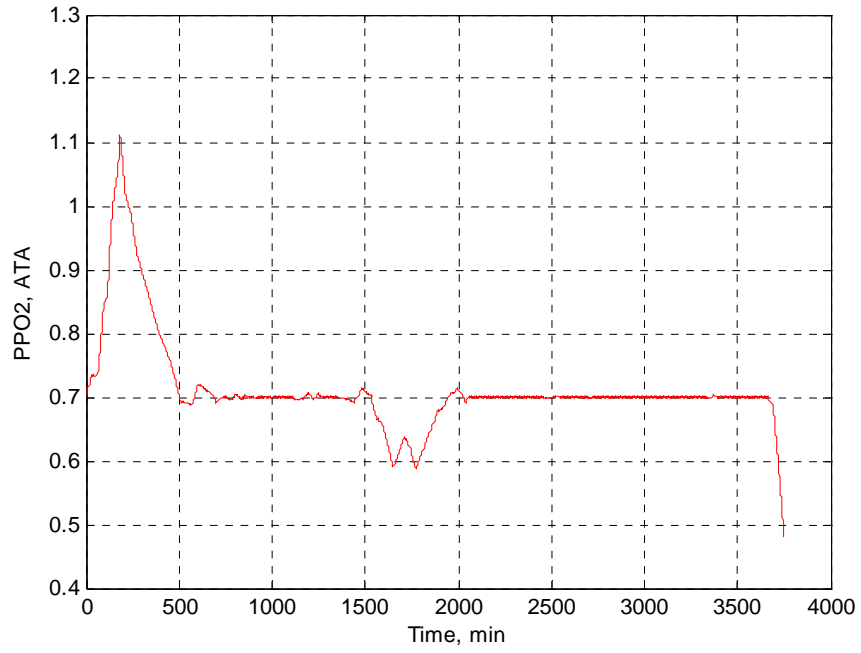


Figure 6-20. PPO2 in the breathing loop.

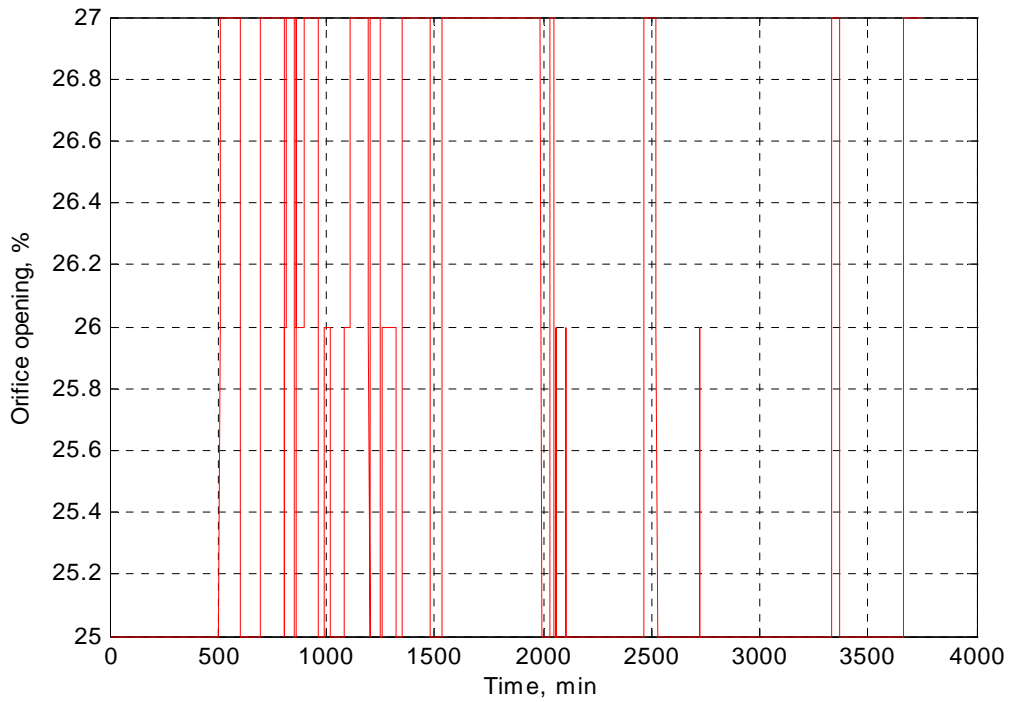


Figure 6-21. Orifice opening.

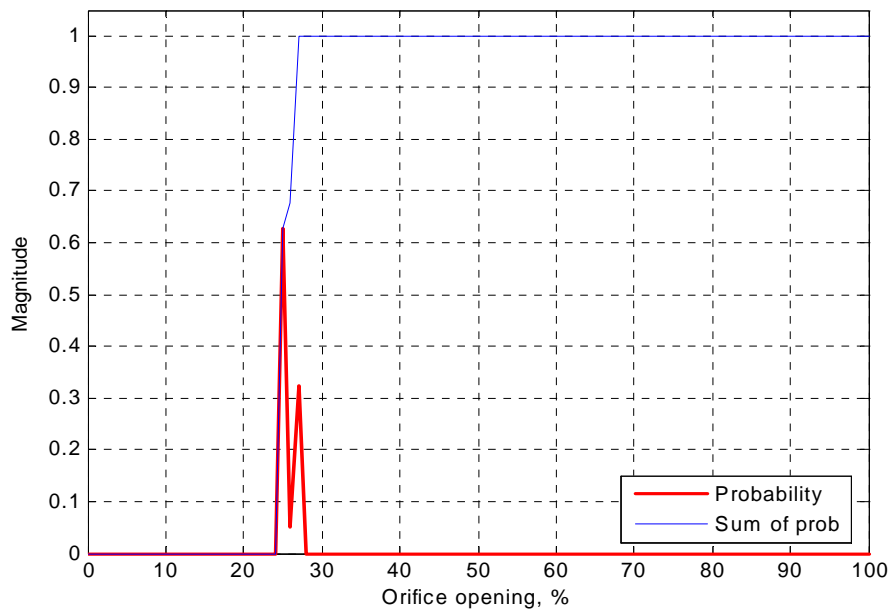


Figure 6-22. Orifice size probability. 100% orifice opening in the range from 25 to 27% that corresponds to the O2 injection in the range from 0.973 to 1.135. The fault probability for the depth profile is zero.

7. EMPIRICAL TESTS

Empirical test was carried out samples from a batch of five Deep Life dual scrubber commercial diving rebreathers, shown below. These have two independent rebreather injector systems (two channels), each of which have dual redundancy in their electronics. This case is the worst for testing the orifice safety, because one channel will tend to “fight” the action of the other channel – this is resolved automatically by the channel the tighter tolerance acting as a lead device in controlling the PPO2.



Figure 7-23. The batch of 5 rebreathers from which units (rebreather controllers, and injectors) were selected for the empirical tests, Serial numbers DRB03 to DRB07 inclusive.

Tests were carried out by disconnecting the batteries from the rebreather, then when the rebreather is operating cutting the umbilical power: this causes a very sudden and total loss of all electronics.

Two sets of tests were performed: unmanned and manned.

1. Unmanned testing with a worst case profile: this involved a descent at the maximum possible rate from the surface to 70msw, remain at 70msw for 15 minutes and then rocket to the surface at a rate of 110msw per minute. The total power loss was applied at a depth of 1.3msw on the descent. The make up gas was Nitrox 4 (4% of O₂), and the pure O₂ supply was Nitrox 75 to create worst case conditions for PPO2 control.
2. Manned testing for a diver working hard near the surface in the Norwegian State Dive School in Bergen, who ascends on the breathing loop after total loss of power and all electronics. To ensure the safety of the diver, an independent PPO2 monitor was fitted to the rebreather and standby divers observed the PPO2 monitor which hung freely from the diver, during the ascent on the ladder from Pool Number 1.

7.1 Results of unmanned tests, extreme profile example

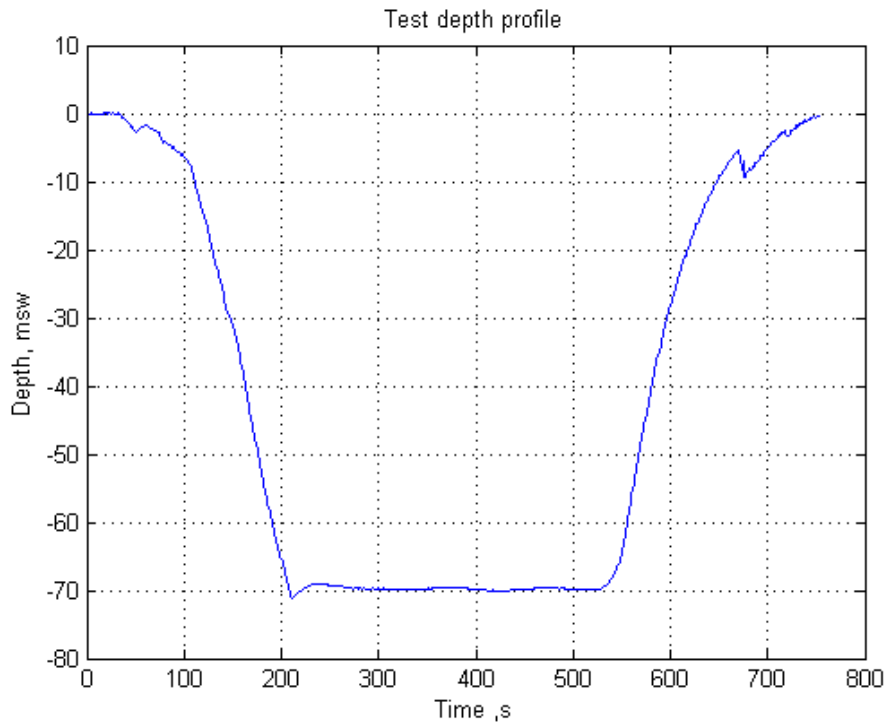


Figure 7- 24: Dive profile used for unmanned testing of O2 orifice failure. This is not a human survivable profile: it is intended to be the worst case for PPO2 control.

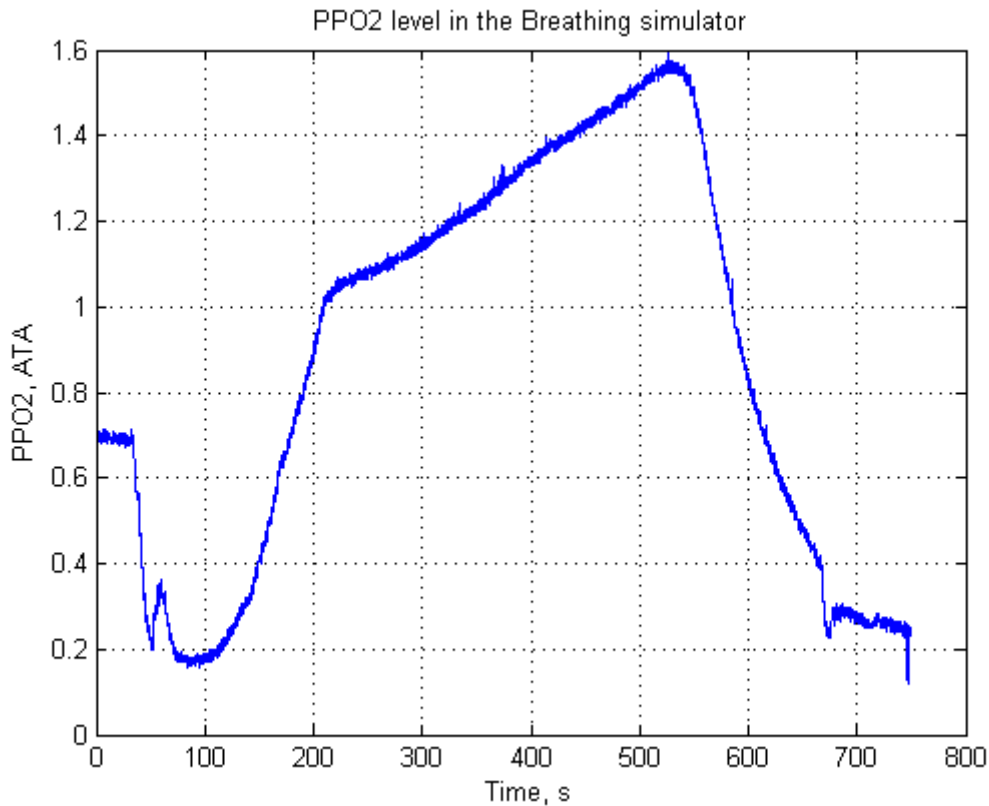


Figure 7- 25: PPO2 plot in the dive with the above profile. Note a PPO2 was maintained of 0.7 until power was removed at a depth of 1.3msw, but the PPO2 remained within safe limits at all times: the spike dip at the very end is a diluent flush.

The above profile is an example. Other profiles were tested. The above case was the worst case, that is, the case that resulted in the greatest PPO2 deviation from the set point.

The equipment used was identical to that reported for the WOB and PPO2 compliance tests for these rebreathers.

7.2 Results of manned test

The complete electronics failure mode was stimulated in Dive 10 in Week 11, 2008 at the Norwegian State Dive school, with a commercial diver from Technip Norge AS. The makeup gas was Nitrox 32 (intended to be the worst case: the minimum oxygen fraction for this depth is Nitrox 60), there was no oxygen supply. The diver was working hard, a complete power loss occurred, and the diver returned to the surface via the ladder. The PPO2 set point was set at 0.3 bar (by use of a test firmware version to over-ride the normal lower limit of 0.7). The PPO2 was dropped from by 0.05 before the diver was out of the water and helmet off. This is a reasonable degree of PPO2 control. However, complete logging was not carried out because there was no electrical power, and no obvious means to do so. An unmanned environment would allow much more extreme profiles to be checked, with full PPO2 logging using the pressure chamber bleed pneumo line.

8. CONCLUSIONS

1. Formal verification confirms that the variable orifice injector can provide a fail-safe oxygen dosing system for a rebreather, to provide sufficient time for a return to bell or for a bail out to staged bail out systems.
2. In the case of a mCCR, such as when a variable orifice eCCR fails, the rebreather should operate as a pure oxygen rebreather when closer than 6m to the surface.
3. When variable orifice dosing valves are used in an eCCR or eSCR it is possible to reduce the risk of a failure occurring when the orifice is in an abnormal state can be reduced, generally to zero, if orifice position limiting is used by the controlling firmware. Formal modelling of the Deep Life Orifice Limiting algorithm shows that this limiting does not cause unacceptable fluctuations in PPO2. The orifice limiting algorithm is simple to apply, and is therefore an ALARP good practice. The safety standards may need widening to allow PPO2 to vary by up to 0.2 from set point in the general case, but it is possible to meet existing regulations with a 0.1 set point variance.
4. Empirical testing shows that the diver can survive a complete dive with orifice failure, under very severe conditions. It is not possible to test every possible combination of dive profiles and gases, so the diver should bail out when such a failure occurs to remove all risk completely.
5. A solenoid based oxygen dosing system would not have maintained the PPO2 within limits needed for human life under the test conditions. The variable orifice valve is a key element of the safety system, reducing considerably the reliance on rebreather power under failure conditions.

CREDITS

Credit and our thanks are especially due to Kåre Segedal of the Norwegian Underwater Institute, for identifying the need for formal modelling of this case in a HAZOP Study, sponsored by StatoilHydro Norway and Technip Norge AS.