Oxygen Cell Fault Data for Assessment of O2 Sensor Fusion Algorithms and PPO2 Controllers

DOCUMENT NUMBER: [Filename]	Test Data for Sensor Fusion Algorithms RV 130325.doc
CONTRIBUTORS:	**Dr. Bob Davidov, Dr. Alex Deas**
DEPARTMENT:	**Verification**
LAST REVISED:	**25th March 2013**
REVISION:	**A0**

APPROVALS	
____/AD/_____ Project Leader	__**25th March 2013**____ Date
____/BK/_____ Quality Officer	__**25th March 2013**____ Date

Controlled Document ☒ Classified Document ☐

DO NOT COPY.

Revision History

Revision	Date	Description
A0	25th Mar 2013	Taken from O.R. Project test harness for purposes of publication to promote good practice.

Quality High Integrity Environment

Certified IEC EN 61508
Compliant at SIL 3

Table of Contents

1 Purpose and Scope

The purpose of this document is to describe the critical test cases used by Deep Life in evaluating oxygen Sensor Fusion Algorithms (SFA) to determine the PPO2, and PPO2 control algorithms, to ensure they are stable and maintain the diver's safety under fault conditions. The purpose of the publication is to enable these cases to be reviewed and to promote good practice in the industry.

Galvanic oxygen cells used in rebreathers are delicate so are easily damaged. Even under ideal conditions the cells have a short working life: just 18 months from the date of manufacture. Oxygen cells fail frequently, and common mode failures affecting multiple sensors occur frequently. The cells are co-located within a rebreather so if the cells in the rebreather are abused by being exposed to cold, heat, mechanical shock, rapid decompression, condensation or contamination, then multiple cells may fail simultaneously and in the same manner. The sensor fusion algorithm in the rebreather must tolerate these failures, through a combination of cell screening, design of the cells to maximise the probability of failing in a particular mode when a failure occurs, and recognition of faulty behaviours.

The tests cases are derived from empirical test data and accident analysis. The test data generally comprises a pair, the first of which displays the fault of interest is exhibited and the second creates the worst case of that fault class by adjusting the test data.

Deep Life carried out an 8 year characterisation study of oxygen cells, a summary of which is published [1]. During the study, Deep Life worked closely with leading manufacturers of oxygen cells to create a cell suitable for rebreathers which is as rugged as reasonably possible, eliminates many fault modes, improves reliability and increases the probability of failing in a known state (output low), compared to cells in common use. However, despite these efforts the oxygen cells remain the least reliable part of a rebreather. The test cases are specific to these Deep Life cells: cells that are not optimised for rebreather applications have additional failure modes which should be added to these test cases should they be used in any application.

The scope of this report is presentation of test data as part of a test plan for a SIL 3 safety critical system.

2 Exhaustive analysis

All Deep Life sensor fusion algorithms are tested with exhaustive analysis of inputs, to ensure there is no unstable behaviour. This is performed in two phases:

1. Each cell input is scanned over the range 0 to 3 bar in 50mbar increments. The huge amount of data these scanning tests create are reviewed as colour cubes, where the output from the algorithm is mapped in 3D into a colour spectrum.
2. Monte-Carlo methods (randomised input) is used, to achieve full Statement, Condition, Branch and Term fault coverage. The output is verified as 3D colour maps.

The use of the fault models in this report is in addition to the exhaustive analysis of the oxygen sensor fusion algorithm, and is applied after the exhaustive analysis to ensure that the algorithm being tested is correct and operating in the manner intended.

Deep Life's sensor fusion algorithms are written in SPARK Ada, for which formal coverage and verification tools are available. SPARK Ada in the Carnegie Mellon PPS methodology used by Deep Life achieves better than 1 defect per 10 KLOC, and an SFA is typically 300 lines of code therefore a

SFA has a 3% chance of containing a bug prior to verification, including the application of these test cases. However the prime purpose of the empirical test cases and the exhaustive analysis is not to verify the code is bug free but to validate the operation of the algorithm to ensure that it does what is intended and does not suffer from a susceptibility to identified failure patterns and modes.

3 Cell faults are often not random and not singular

Oxygen cells in rebreathers cannot be considered as random failure events: most failures are not random but due to abuse of the sensor, or manufacturing fault in the sensor, and that abuse occurs to all the sensors simultaneously.

- For example, if a rebreather is transported on the floor of a Rigid Hull Inflatable Boat (RHIB), driven at for example, 50 knots – not uncommon for a RHIB, then it will suffer severe mechanical shock, far beyond the design limit for the oxygen cells.
- Another example, if the rebreather, usually black, is left out in the sun in a tropical location, the temperature the cells are exposed to will probably rise well above their 45C limit, and as a result they will be damaged – losing electrolyte. All those damaged cells with suffer a further common mode failure mode when the diver starts diving, plunging the rebreather into cold water, with the temperature compensation on the cells (with its 30s response time) failing to track the actual electrolyte temperature within the cell (with is 700s response time). The converse example is also true, where a diver goes to a cold location, the cells are exposed to temperatures below freezing, damaging the cell, then goes diving.
- Rapid decompression causes temporary faults in oxygen cells, affecting all the cells in a similar manner.
- Even ageing is not a singular event: many divers fit cells from the same batch, which will suffer ceiling faults at the same age. This has resulted in fatal accidents.

Due to the high frequency of these multiple failures – multiple cell failures are a frequent event, and the abundance of common failure modes, adding more and more cells to a rebreather does not in itself increase availability of working cells: it actually reduces the overall reliability as more cells will fail in a given time period, and can overwhelm the fusion algorithm with data from common mode failures.

For these reasons, it is necessary to consider both single failures and plural failures, minority failures, and majority failures. A single failure is always a minority of the cells, but a plural failure may be a minority or a majority, depending on how many cells fail and how many cells are fitted to the equipment.

The most probable root cause of a significant number of the fatal accidents in the rebreather accident study can be traced to two of three cells failing simultaneously, usually with a ceiling fault. It is absolutely vital that the sensor fusion algorithm tolerate this type of failure and handle it safely. In particular fusion algorithms based on the correlation of a pair of sensors, such as "voting logic"*, are dangerous when used with a rebreather.

* "Voting logic" in this context has little in common with digital voting logic used to identify faulty computers in, for example flight controllers. In a rebreather "voting logic" refers to algorithms that select the closest two sensors, check the sensors are within 10%, and take the average, rejecting the third sensor. As sensors generally fail low, voting logic will frequently follow the two faulty sensors when two faults occur, with likely fatal results. It is the unsuitability of voting logic in this application that gives rise to scientifically derived sensor fusion algorithm for test using these test sets.

4 Empirical Test Cases

The empirical test data presented herein was gleaned from:

1. FMECA studies,
2. Extensive Oxygen Cell Characterisation identifying fault modes which are then recreated to give true empirical data,
3. Test Data during rebreather testing,
4. Accident analysis and log recovery.

Unless stated otherwise the file containing the fault data is O2CellFault_xxpyy_YYMMDD.xls
For example, fault mode 3.8 is O2CellFault_3p8_(datecode).xls

4.1 Short Circuit: Stuck at Zero

Cell output is zero, e.g. due to a broken wire, or faulty connector.

4.2 Open Circuit

Cell output is at ADC bias.

4.3 Cell Resistance Fault

Cell has the wrong gain: this means it has a different output resistance than expected.

4.4 Humidity or Pressure Fault

Cell was calibrated when the pressure sensor or humidity sensor was faulty.

4.5 Cell Charge Conversion Fault

This can be tested either by measuring the change in output when a known gas is applied, or by applying a known charge and testing the response in a test gas. This is a cell screening check.

4.6 Calibration Fault

If the cells have been calibrated on the wrong gas, then all cells will show a scaling fault, i.e. the output will be of the form k*PPO2, where k is a constant that is not 1.0. This fault is one that is screened by obliging the diver to verify the calibration using a check gas. For example, calibrating using air can be checked using pure oxygen, with compensation for altitude, humidity and temperature.

The reason for choosing air as the calibration gas and pure oxygen as the check gas is that this combination allows failures in humidity or pressure sensors to be detected: use of pure oxygen for calibration does not provide that integrity.

4.7 Sensor ceiling fault, singular, and Test to ensure Max PPO2 displayed correctly

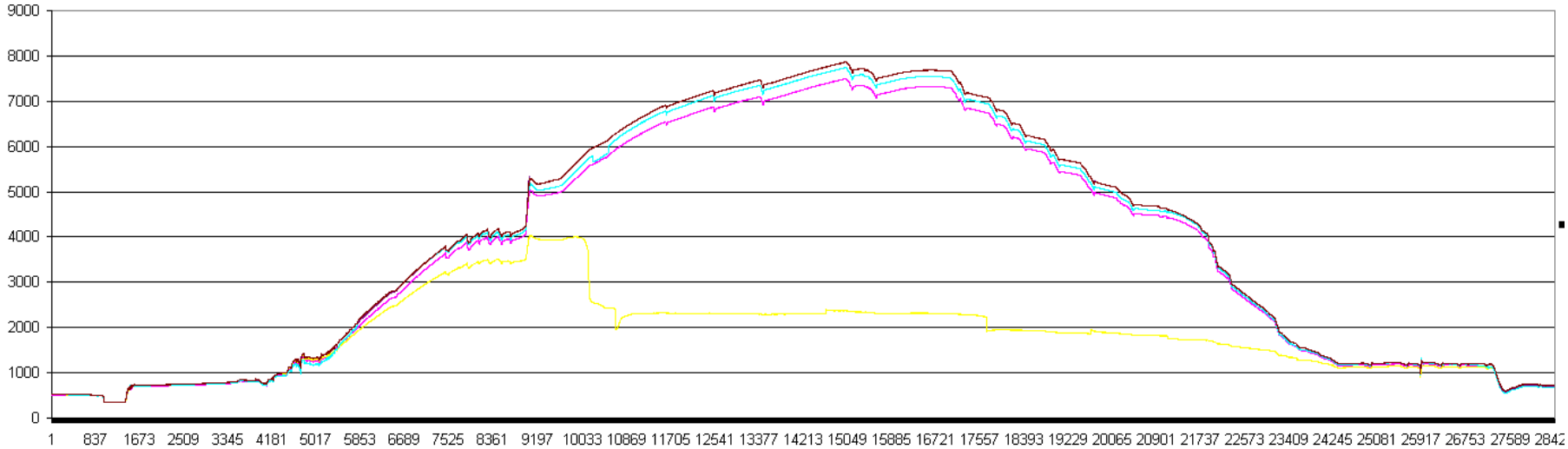


Figure 1. In 3 hour bottom time in test chamber with Mass Spectrometer verifying the black sensor was correct throughout the test. Three Aii cells achieved linearity to 8 bar even when two years old! File: Base_d5_0016-D1_20101220_064356.log_0.xls

4.8 Sensor ceiling fault, plural majority

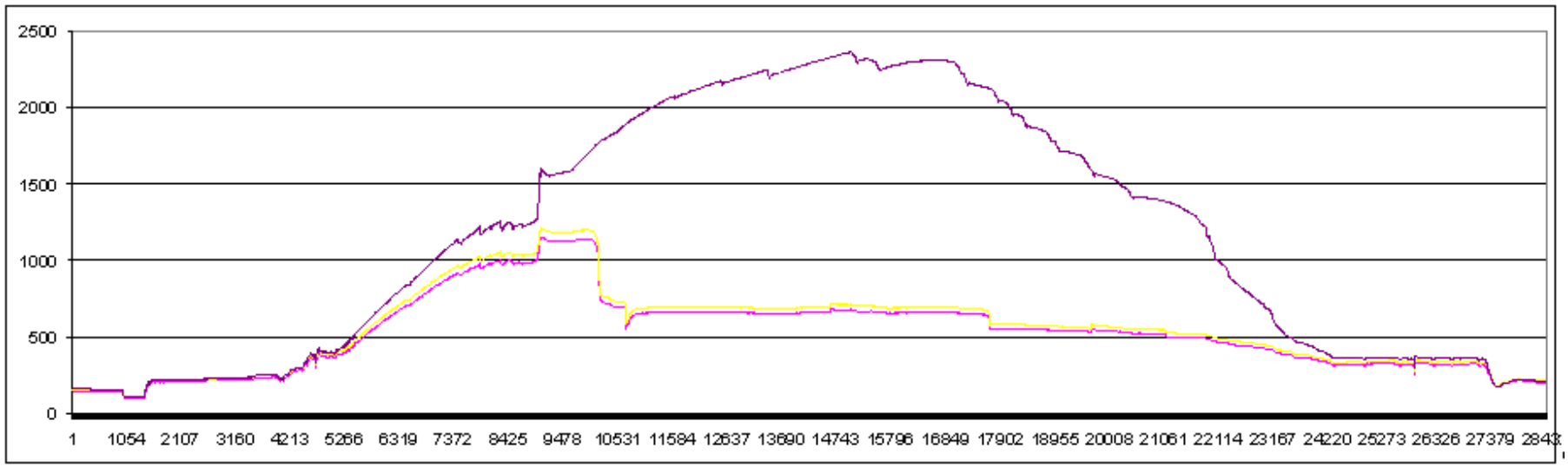


Figure 2. Created artificially by edit of case 4.7 above. File for the above fault is Base_d5_0016-D1_20101220_064356.Artlog_0.xls

Accident investigations have identified that the multiple sensor ceiling fault has occurred several times in third party rebreathers with fatal outcome. The incidence of this fault is high because the normal failure mode of the sensors is a ceiling fault, and with good quality control during cell manufacture, cells from any batch will fail very closely together in time. Diving with out of date cells will lead to this fault, as does abuse of the cells from heat, cold, shock, etc.

4.9 Sensor condensation fault, plural majority

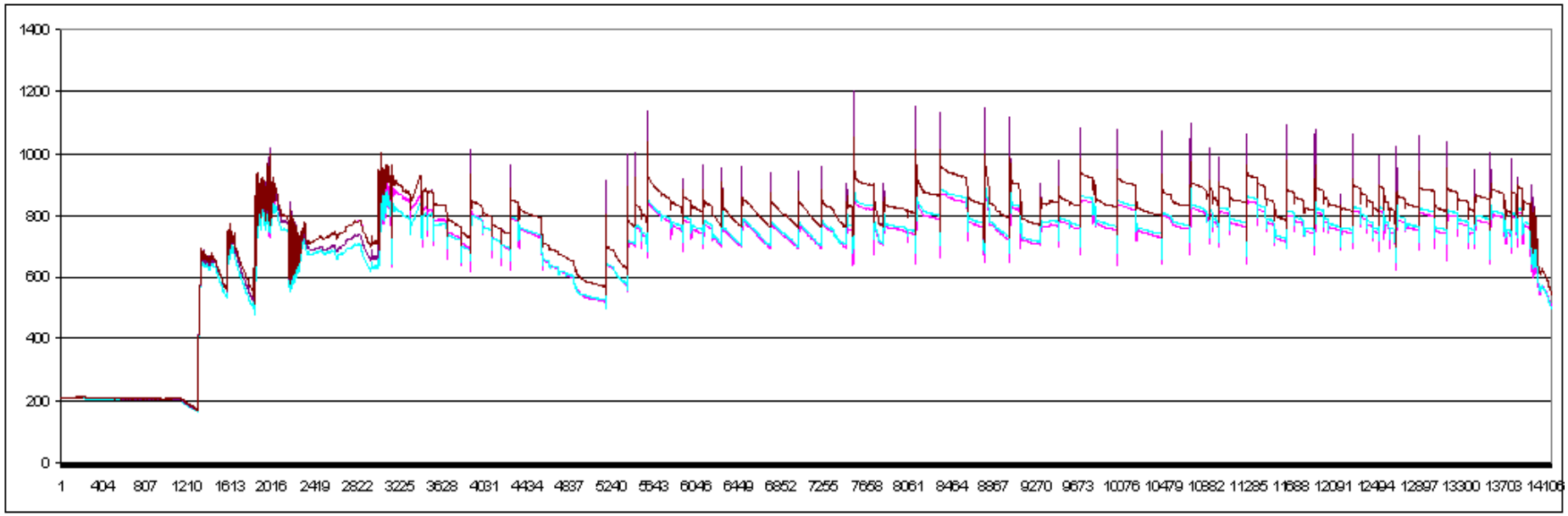


Figure 3. Fault is condensation on all sensors except the brown creating an error increasing with time. The pink sensor drops from the highest position at the beginning of the test to the lowest position at the end of the test. Datafile: out1-101019_040909.bin_0.xls

In the worst case version of the above fault it becomes a ceiling fault indistinguishable from the previous test case.

Note during dive tests, another very serious version of this fault was observed whereby all three sensors in a PPO2 cell holder mounted into a counterlung developed a vapour block during which all cells indicated a steady 0.7 atm when actual PPO2 fell to 0.21atm or below: the fault persisted for around 5 minutes even after the cell holder was removed from the rebreather and exposed to air. The fault mode could not be reproduced: its most probable cause was eliminated by changes to the mechanical arrangements around the sensor, removing the well around the membrane, placing the sensors on the outlet to the counterlung and inclining the sensors.

4.10 Sensor Cross-Correlation Instability, Plural Majority

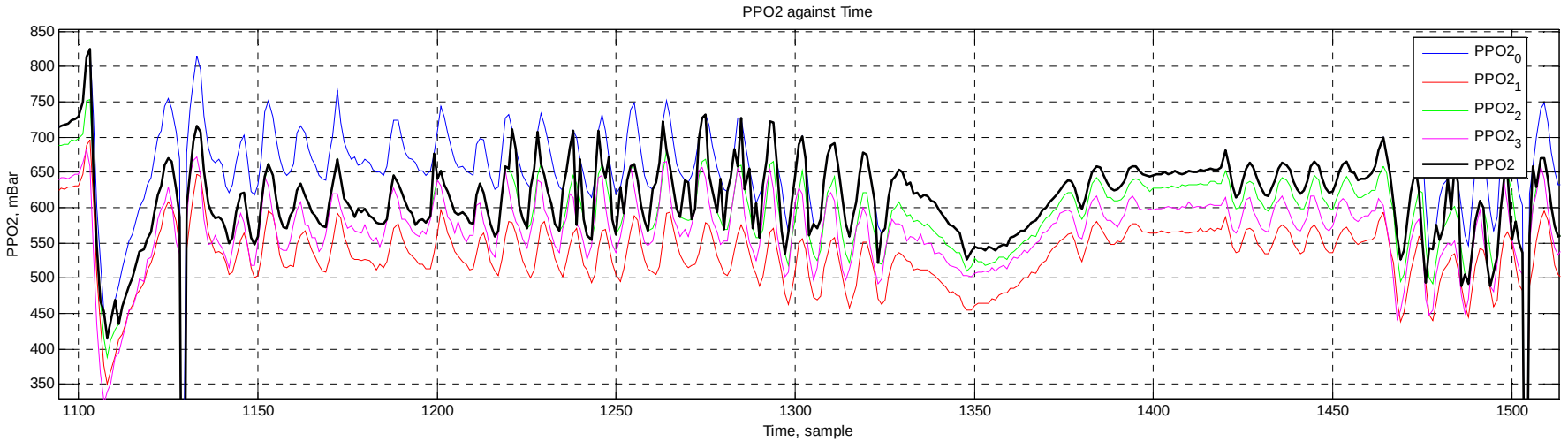


Figure 4. Where the PPO2 is genuinely cycled, sensors vary their relation to the actual PPO2 over time. In this test set, the actual PPO2 (measured using a mass spectrometer, black), does not have a fixed percentage band relation with any sensor, nor does any sensor have a fixed band with any other sensor. This test set is included to ensure the sensor fusion algorithms do not produce results that switch rapidly from sensor to sensor: such a response can cause instability in a PPO2 controller, as the reported PPO2 will change very rapidly, or oscillate, between two levels, and the controller will try and correct for that oscillation.

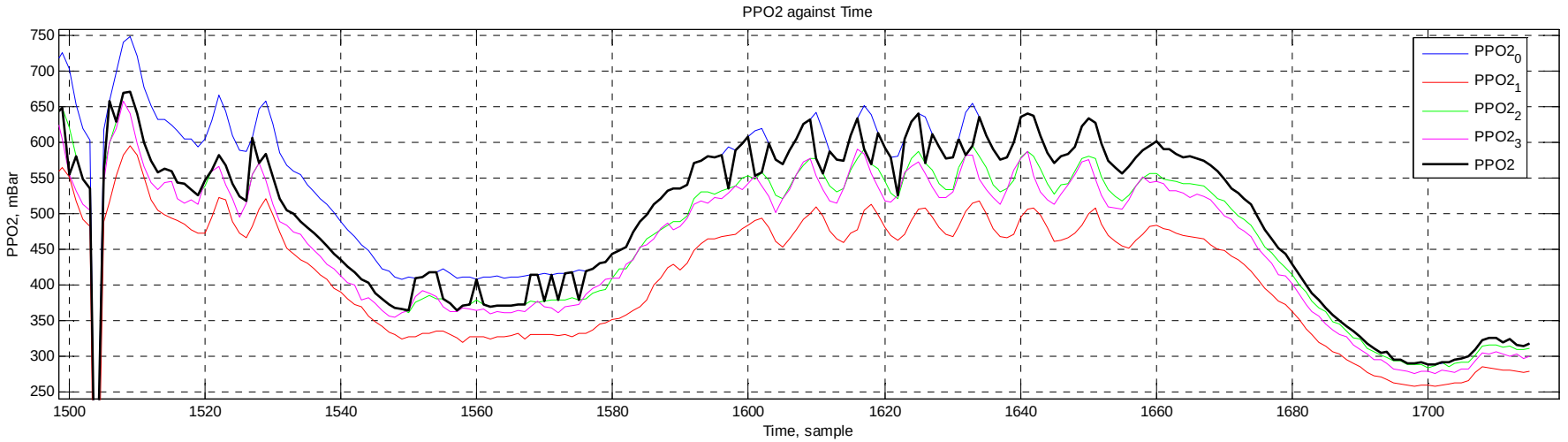


Figure 5. Example of incorrect sensor fusion generating a PPO2 signal that oscillates as the relationship between sensors varies.

4.11 Poor Dynamic Match Fault, Singular Minority

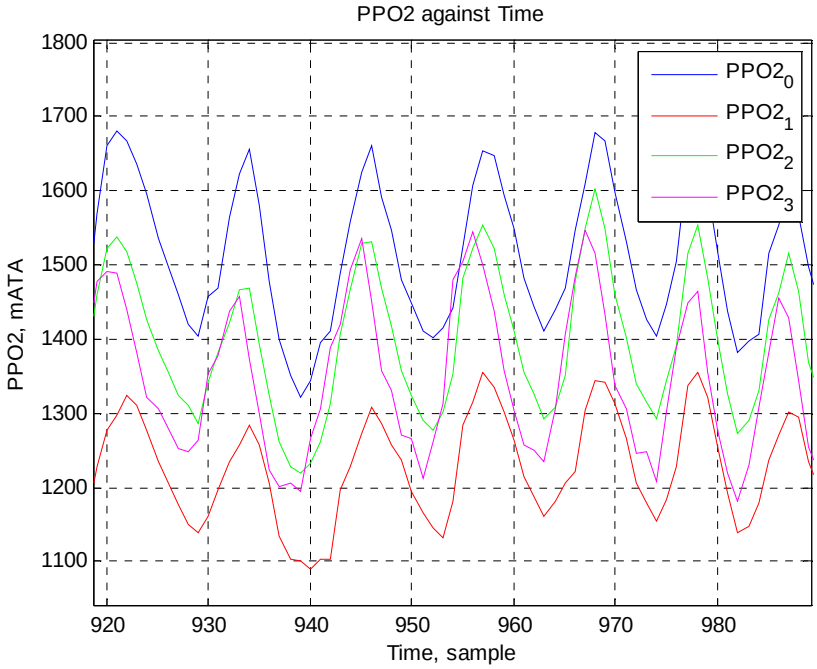


Figure 6. Period is 90 samples, p-p amplitude is ~300 mATA or ~20%; Blue, Green and Purple differ due to calibration, and red is faulty.

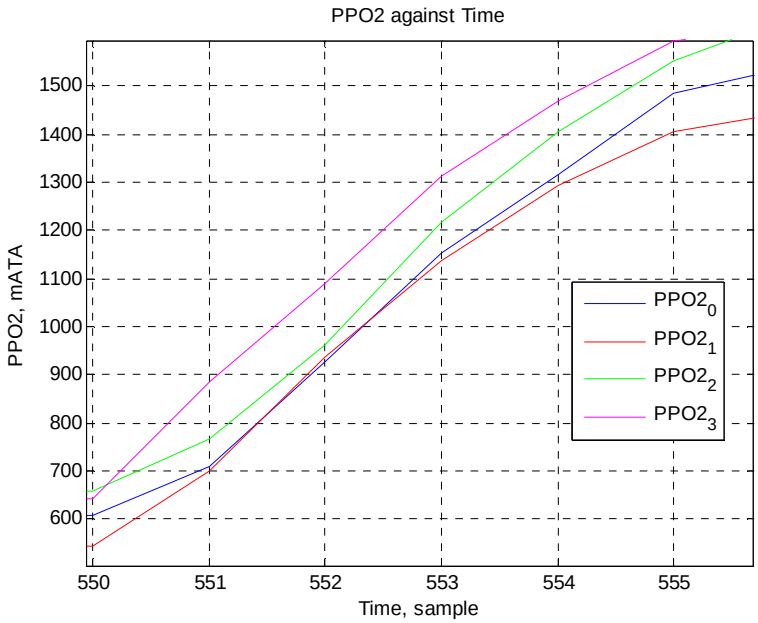


Figure 7. The increase in PPO2 is 900 mATA per 5 samples or 140 mATA/sample;

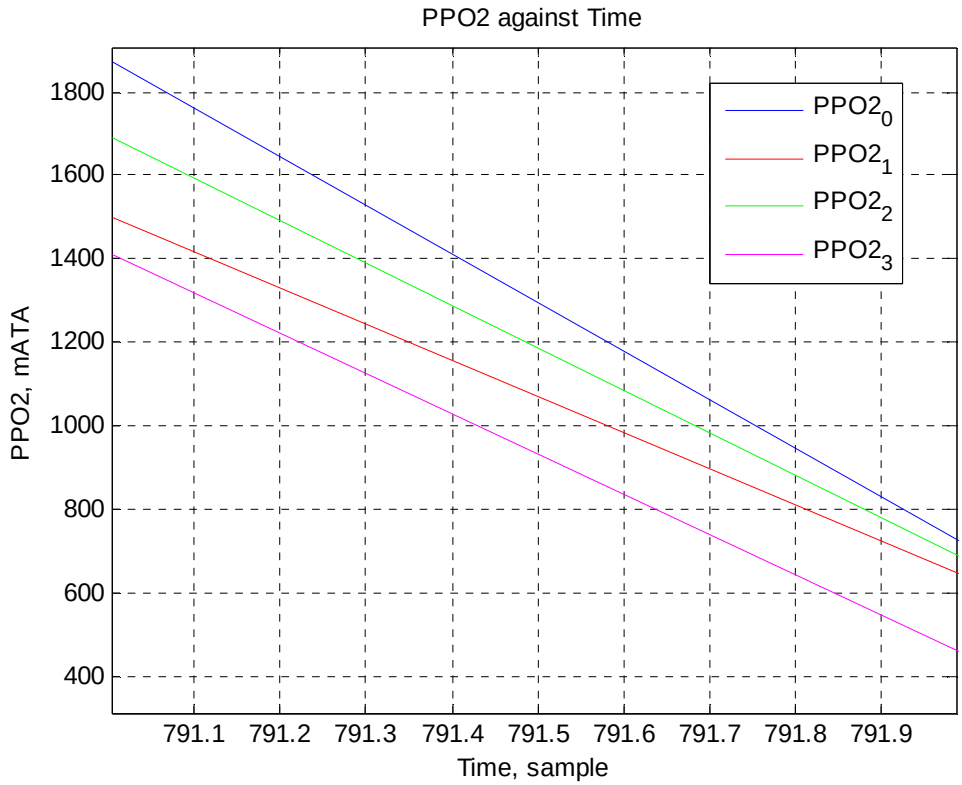


Figure 8. The reduction in PPO2 is 1000 mATA /sample;

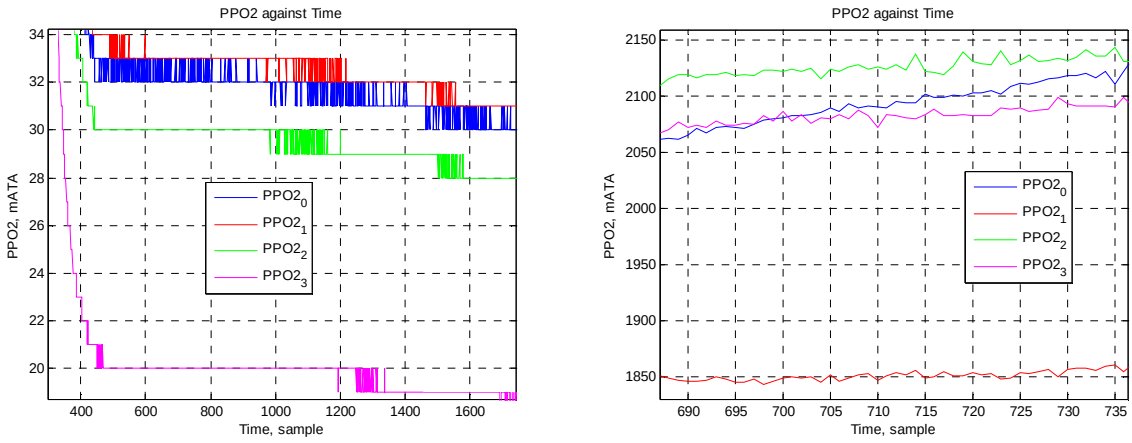


Figure 9. Maximum interval between the sensors outputs; 50% for 20 mATA; 12% for 1850 mATA;

4.12 Stuck At Fault, Singular and Plural Minority

Example given for mid-range stuck at fault, other faults in same class include open circuit and short circuit: all these faults should be masked out following calibration, but are included to test the sensor fusion algorithm's response to the fault should it occur during a dive.

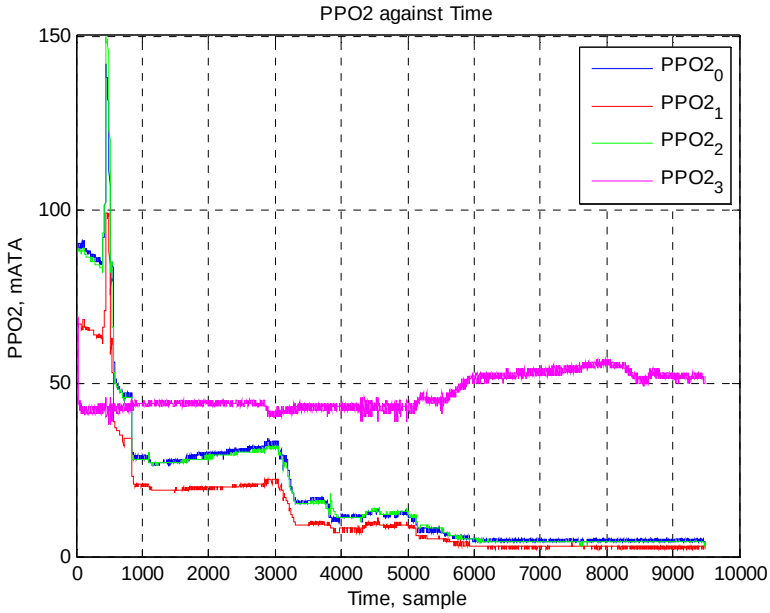


Figure 10. Subcase 1: Cell 3 (PPO23) is faulty or has a faulty ADC channel, with output not correlating to PPO2, additionally Cell 1 (PPO21) has a calibration error.

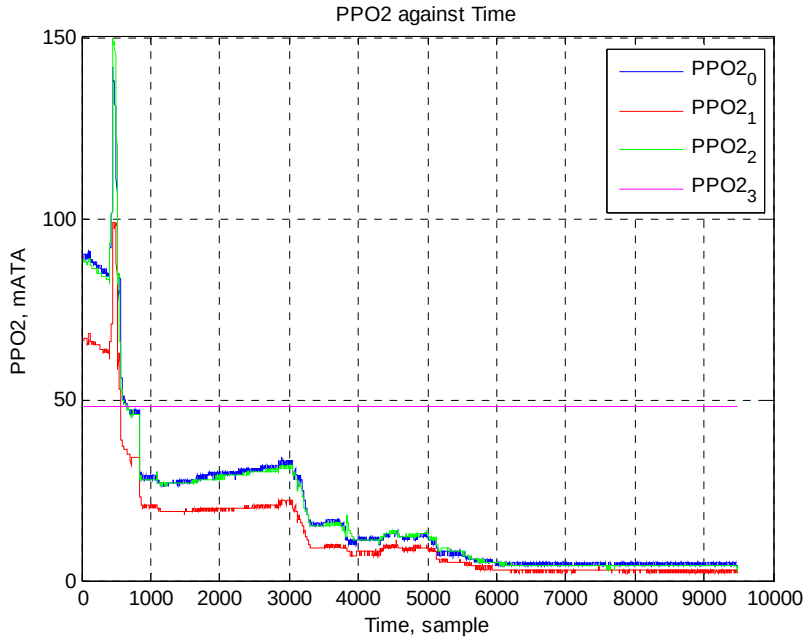


Figure 11. Subcase 2: PPO23 is faulty with stuck at fault, midrange from faulty electronics or ADC.

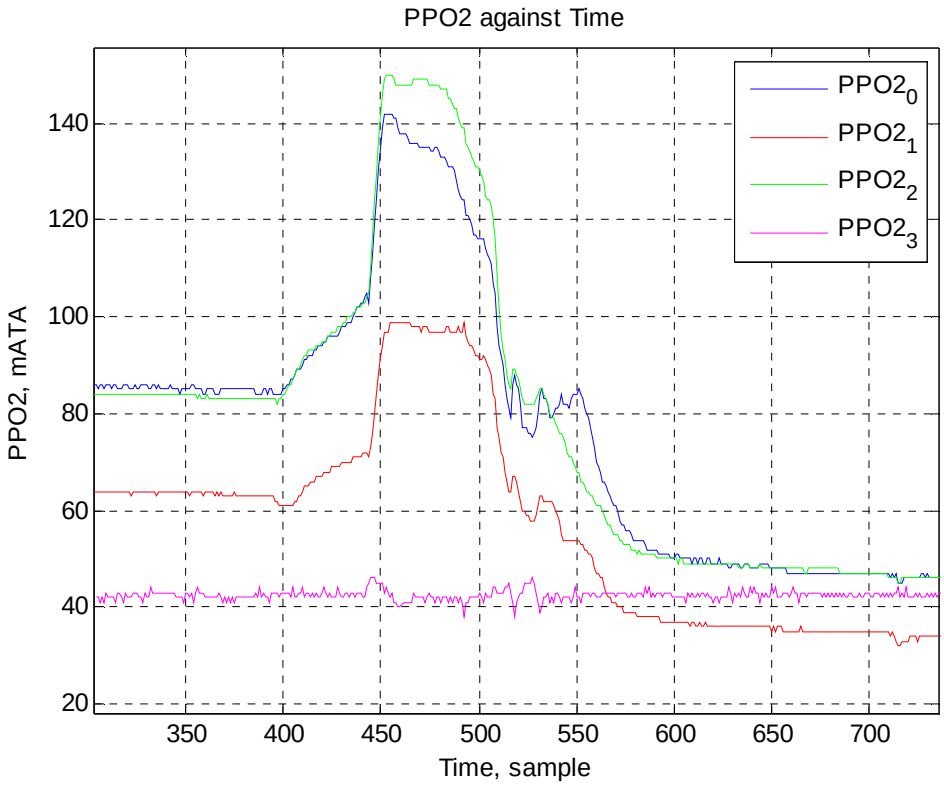


Figure 12. Subcase 3: PPO23 is faulty but becomes close to range of other sensors

4.13 Entrapped Gas Fault, Singular Minority

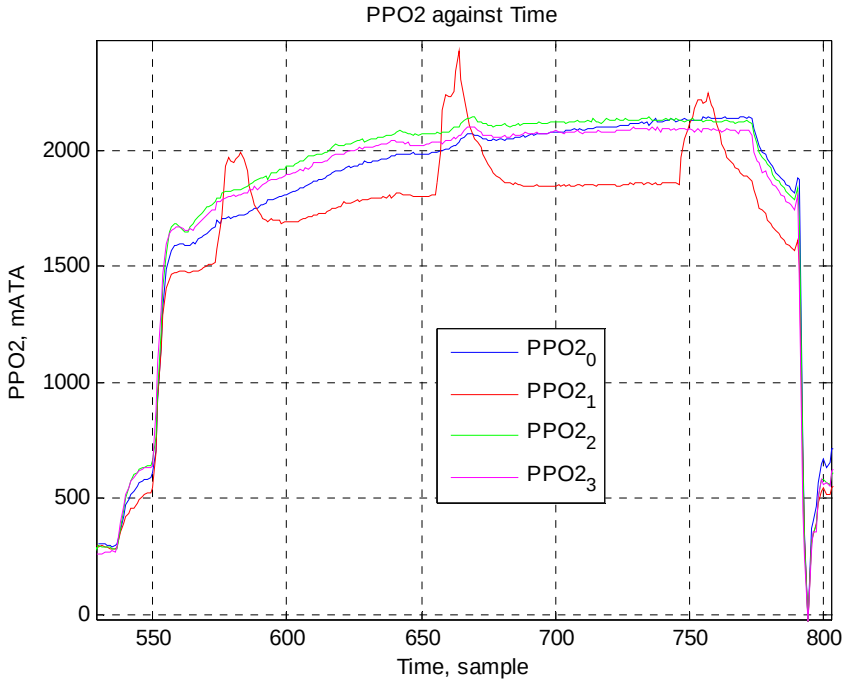


Figure 13. Subcase 1: PPO21 is faulty

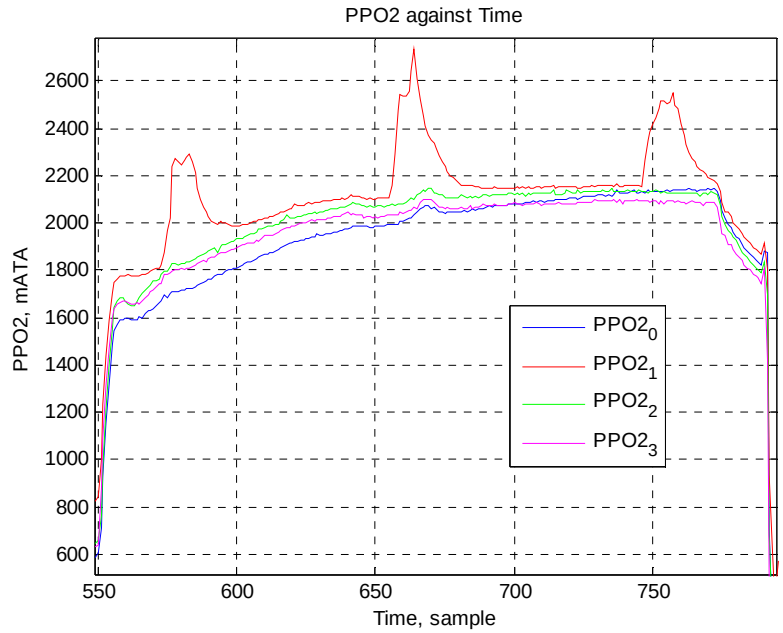


Figure 14. Subcase 2: PPO21 is faulty, created from above to be worst case

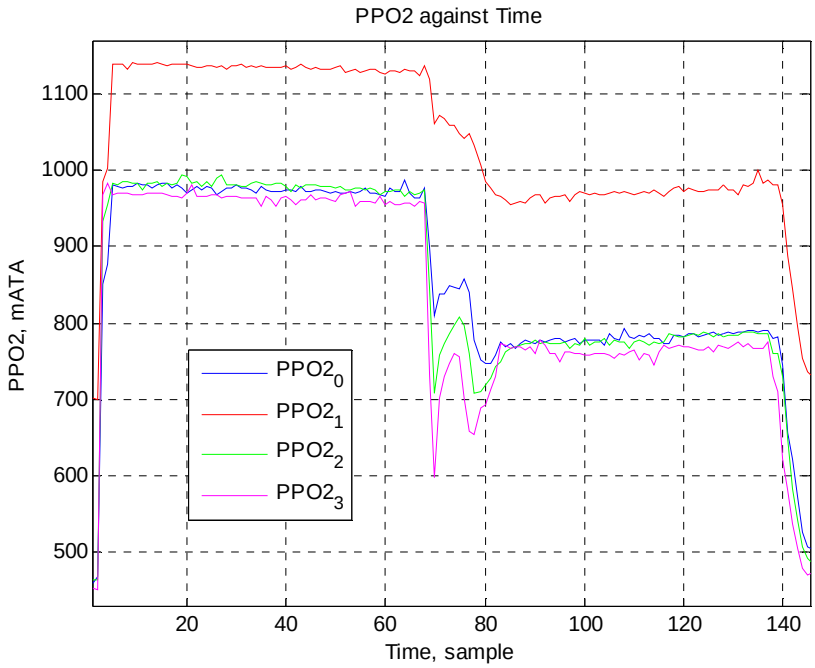


Figure 15. Subcase 3: PPO21 is faulty

4.14 Electrolyte loss - Singular Minority

Electrolyte loss faults can be due to mechanical shock, freezing, overheating or a leak in the housing or membrane. Several mechanical shock causing detachment of the cathode or anode normally cause a zero output.

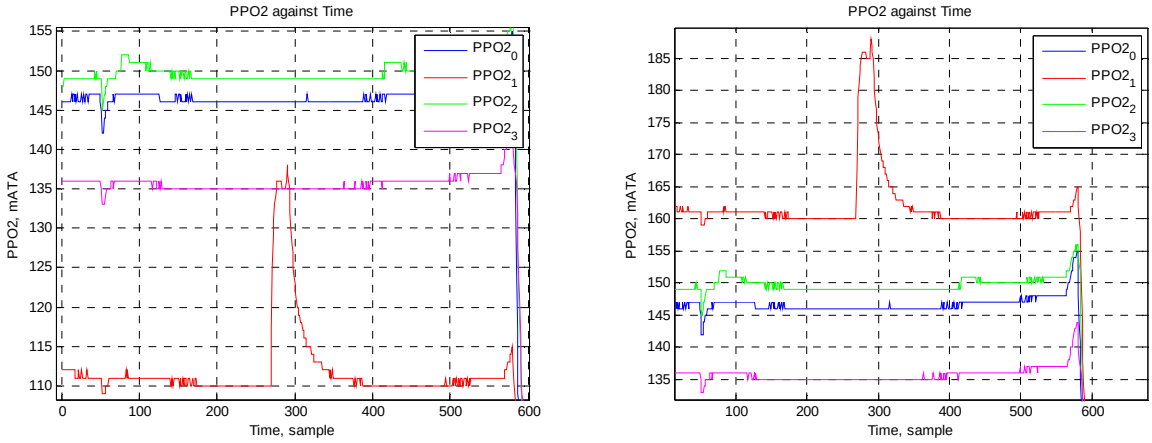


Figure 16. Subcases 1 and 2: PPO21 is faulty, Subcase 2 is worst case produced from case 1

4.15 Electrolyte loss Fault, Plural Majority

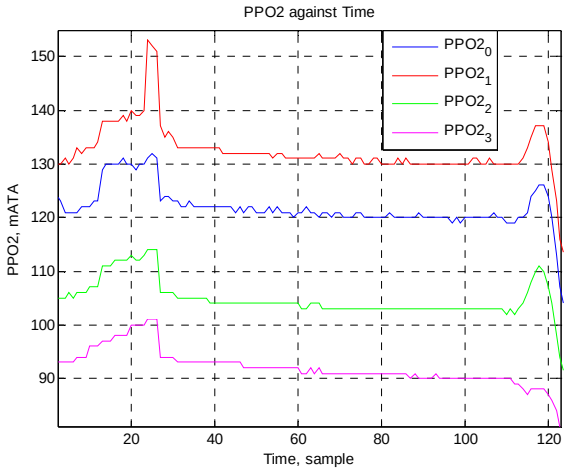


Figure 17. Subcase A: PPO21 is faulty as bubble in electrolyte moves, then recovers. Other sensors are low output due to small amount of electrolyte loss but stable.

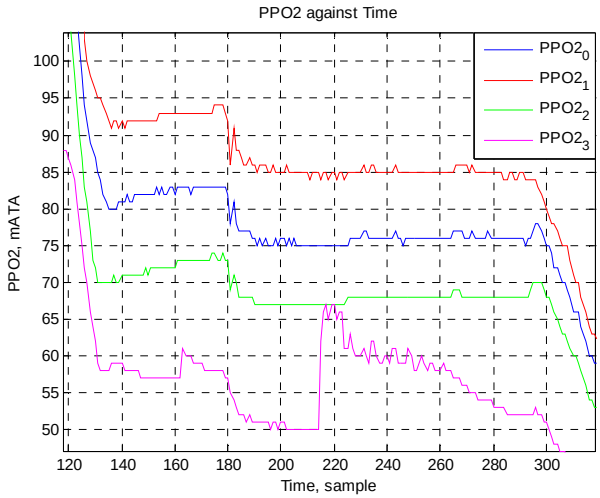


Figure 18. Subcase B: PPO23 is faulty and PPO22 is low.

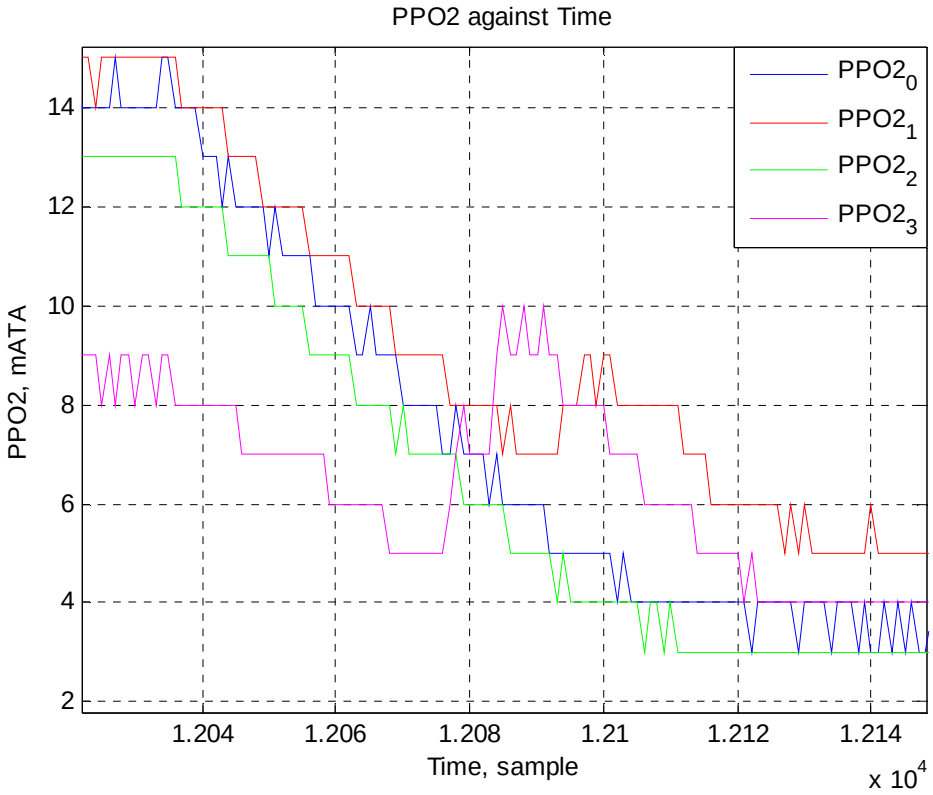


Figure 19. Subcase C: PPO21 and PPO23 exhibit temporary faults.

4.16 Inversion Fault

Extreme Mechanical Shock or Very Fast Decompression can cause the cell output to be inverted (generates negative voltages from the anode).

4.17 Temperature Compensation Faults, Single and Plural Majority

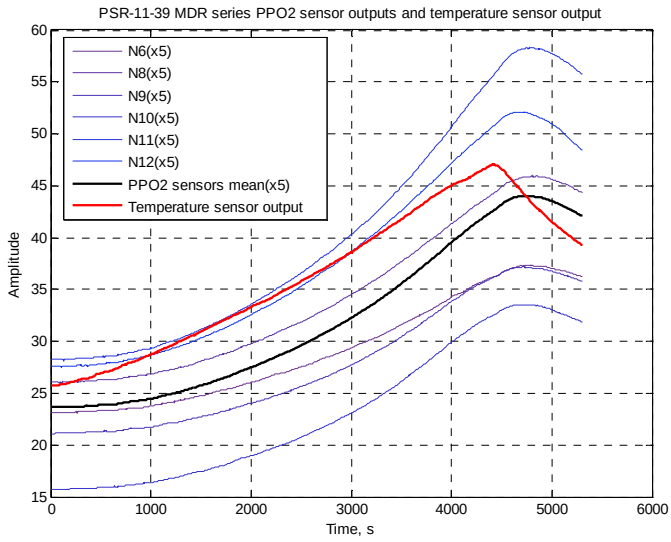


Figure 20. Temperature characteristic from DV_O2_sensor_MDR_temperature_compensation.doc

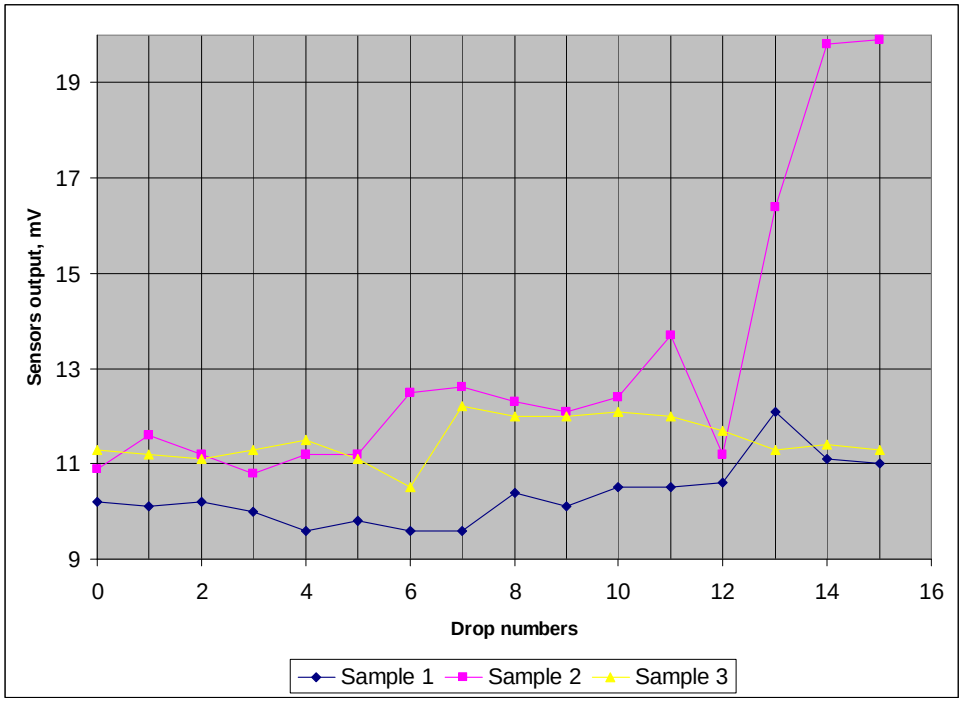


Figure 21. DV_O2_sensor_Teledyne_R22D_070822.doc

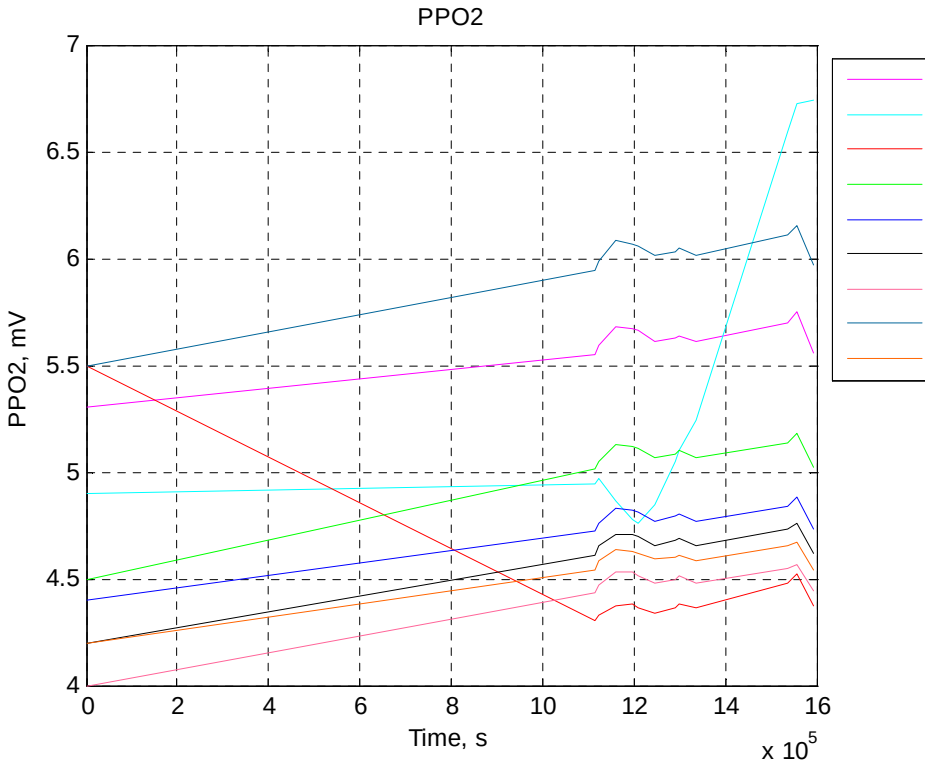


Figure 22. DV_O2_sensor_AII_PSR1139MD_070307_2.doc

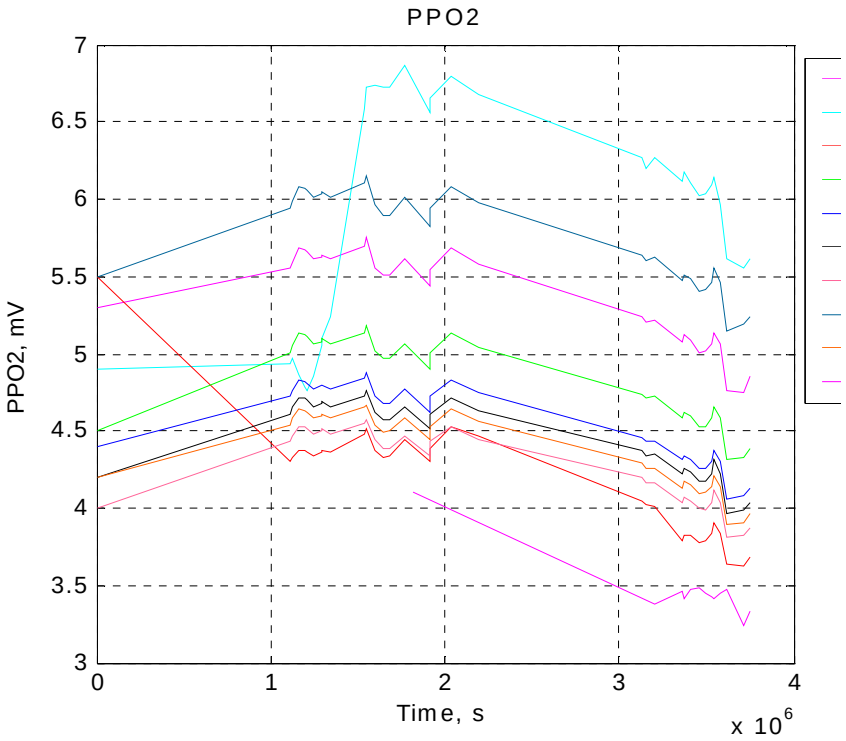


Figure 23. DV_O2_sensor_batch_test_results_061218.doc

4.18 Oscillation Singular, Low Frequency, Minority

.

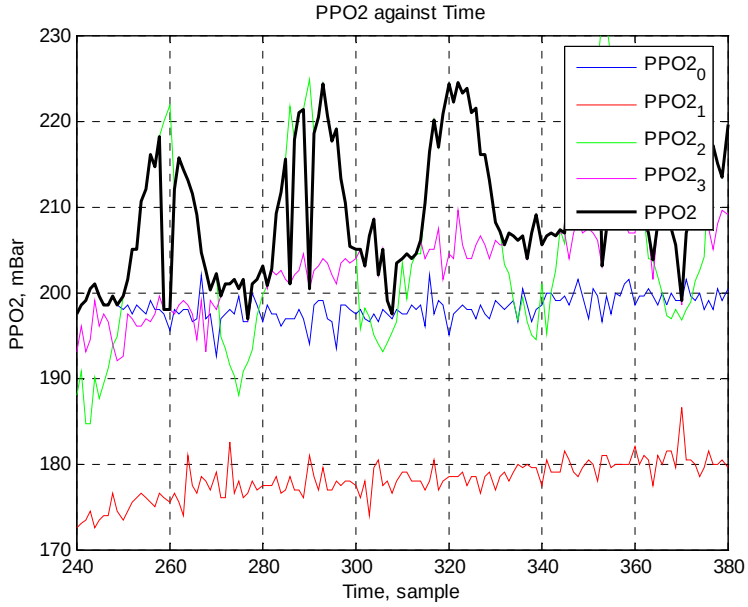


Figure 24. Single sensor has an oscillating output triggered by helium decompression.

4.19 Oscillation Low Frequency, Plural Majority

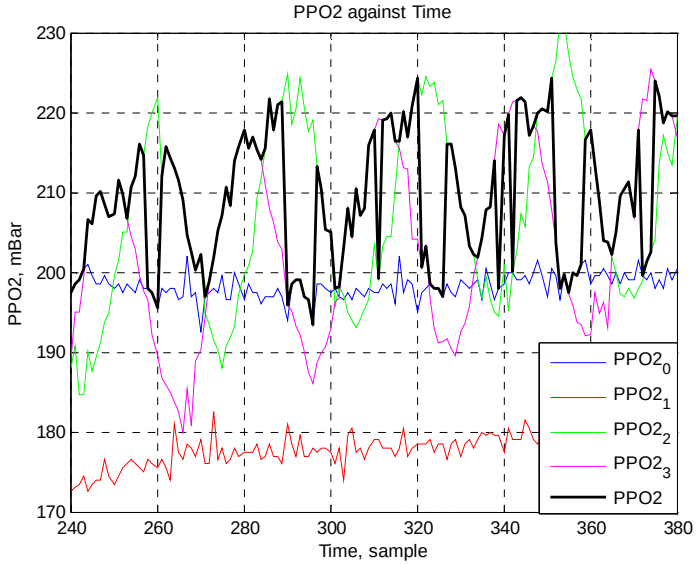


Figure 25. Oscillating outputs independent of PPO2. Black PPO2 trace in this instance is a reported PPO2 and is incorrect: it is included to allow PPO2 controllers to be tested. The cause was an aggressive decompression of the sensors.

4.20 Intermittent Oscillation, Low Frequency, Plurality

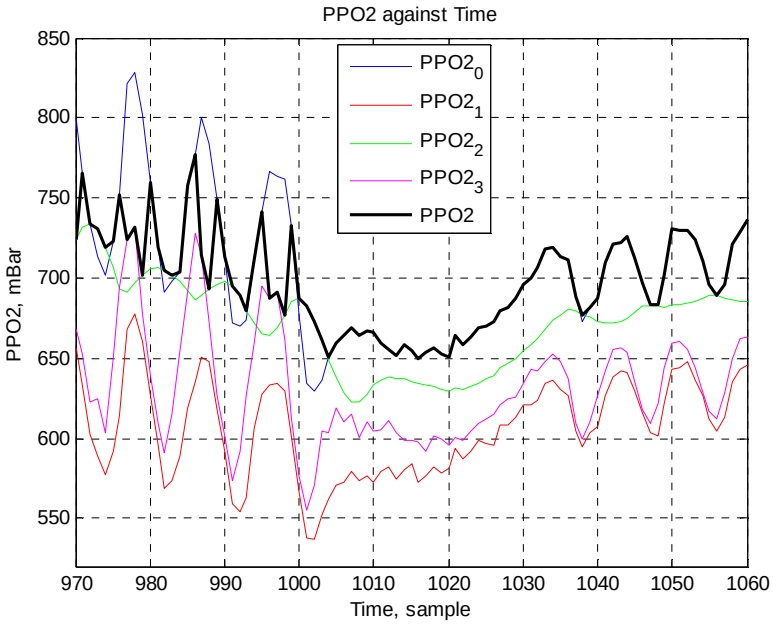


Figure 4-26. Example of sensor bounce identified at the raw sensor data level in test dives, due to bubbles in the electrolyte during the decompression phase of a dive. Sensor 2 in this set has slow response: case below.

4.21 Oscillation, High Frequency, Plural Majority

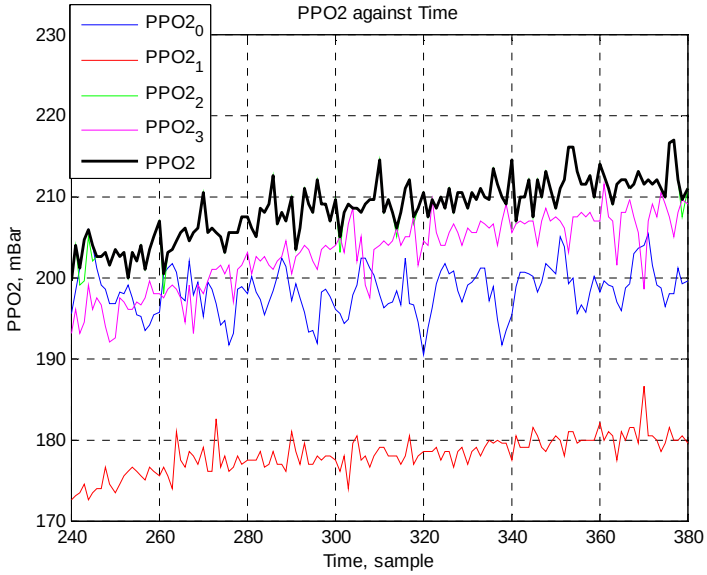


Figure 4-27. Rapid changes in sensor outputs not correlated with actual PPO2 due to very severe decompression gradients.

4.22 Slow Response, Single Minority

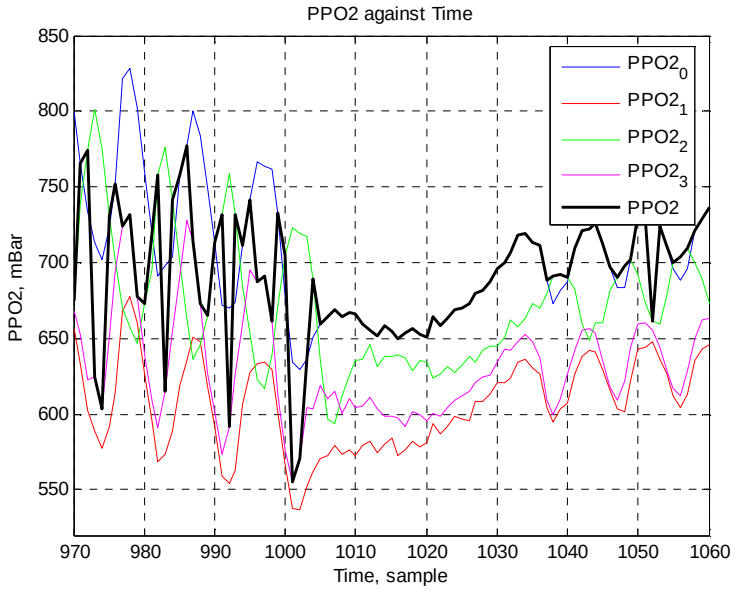
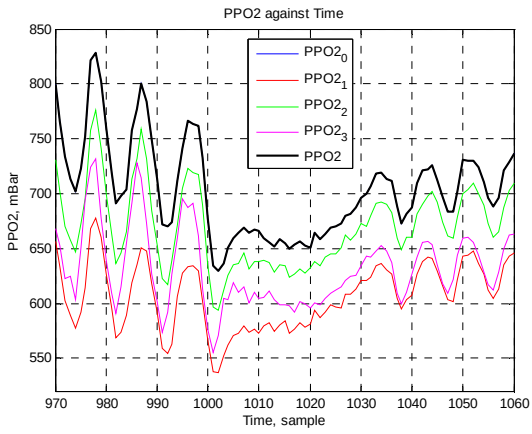


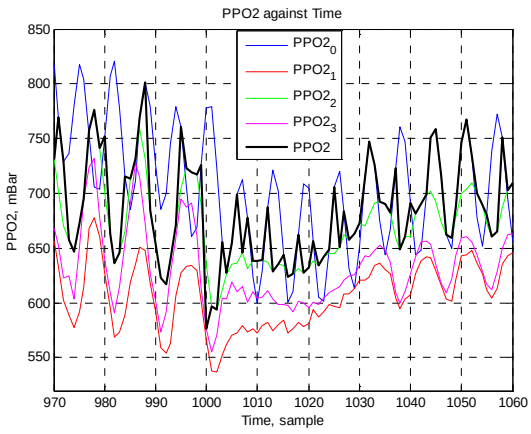
Figure 4-28. Data set 4.20 is same as Intermittent Oscillation set, note the delay in PPO2 response on Sensor 2. Common causes include a vapour block on the sensor, contaminated membrane or blocked membrane.

4.23 FMECA Fault 9.8 (Noisy Output)

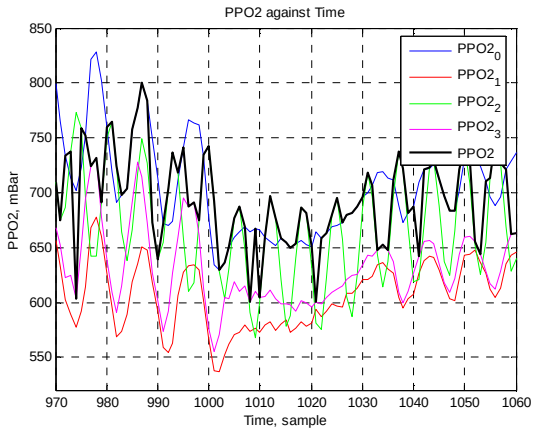
For analysis of the effect of noisy output (where frequency of sensor output changes is higher than rate of change of PPO2), the sensor states shown in the first graph below were used and a noisy output simulated on individual sensors and on different combinations of sensors.



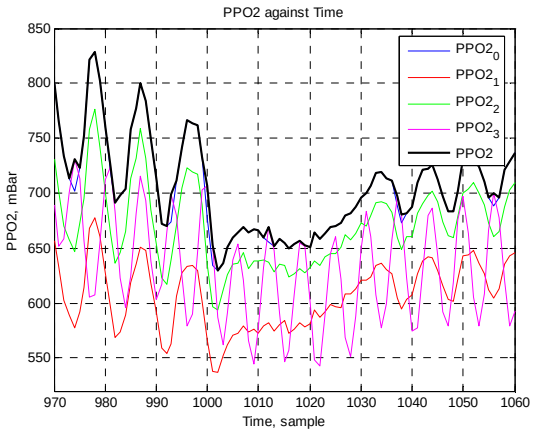
Initial PPO2 in the range of 970..1060s



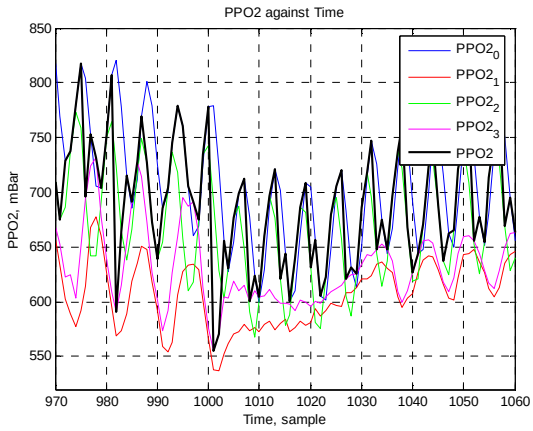
$PPO2_0$ with higher frequency



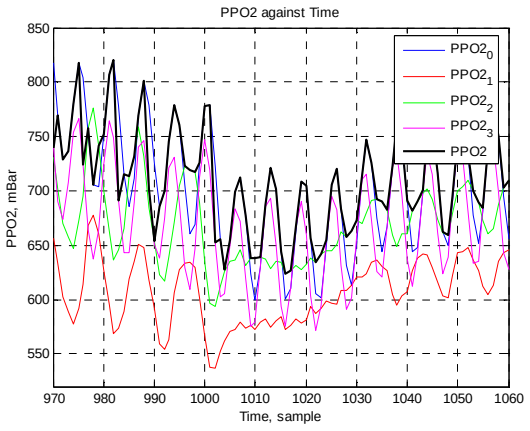
$PPO2_2$ with higher frequency



$PPO2_3$ with higher frequency



$PPO2_0$ and $PPO2_2$ with higher frequency
Phase offset between them is 1s



$PPO2_0$ and $PPO2_2$ with higher frequency
Phase offset between them is 0.5s

Figure 4-29. Noisy output from sensors indicating PPO2 against frequency PPO2i. Frequency of output changes is higher than rate of change of PPO2. Images may be zoomed.

5 Verifying the test data

One danger with test data, is that an engineer may observe a particular relationship within the test data that is true for the test cases but is not valid across all cases in the field. This can lead to the development of a sensor fusion algorithm that is optimised excessively for the test cases rather than considering the base failure modes. To mitigate that danger, tests have been applied to the data to check the data using auto-correlation and cross-correlation functions. An example is shown below, using the data set for a stuck at fault, singular (Test case 4.12, Datafile `'out1-101019_040909_bin_0.mat'`).

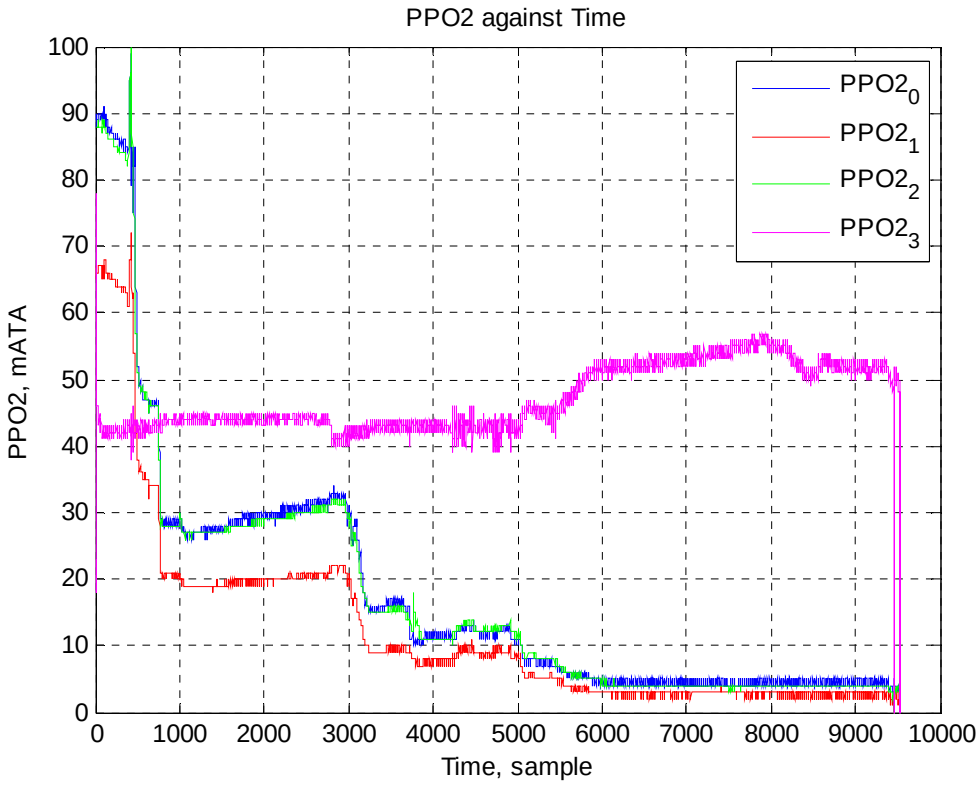


Figure 30. Example of Stuck At Fault, selected to demonstrate the data integrity tests applied to each test case;

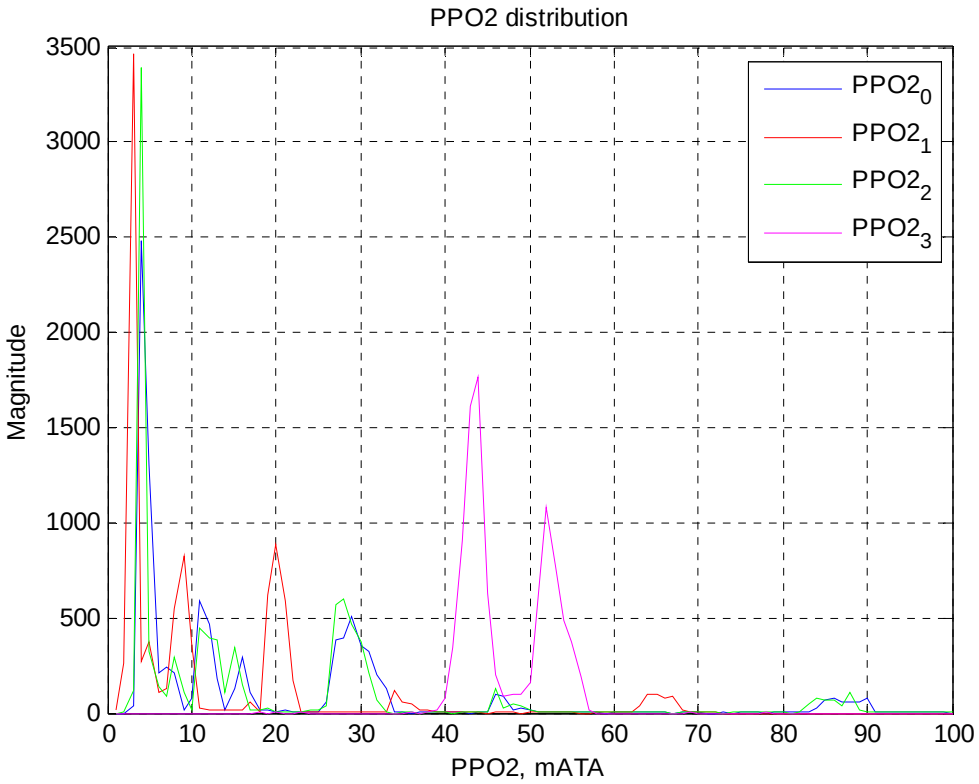


Figure 31. Check on histogram of the test data.

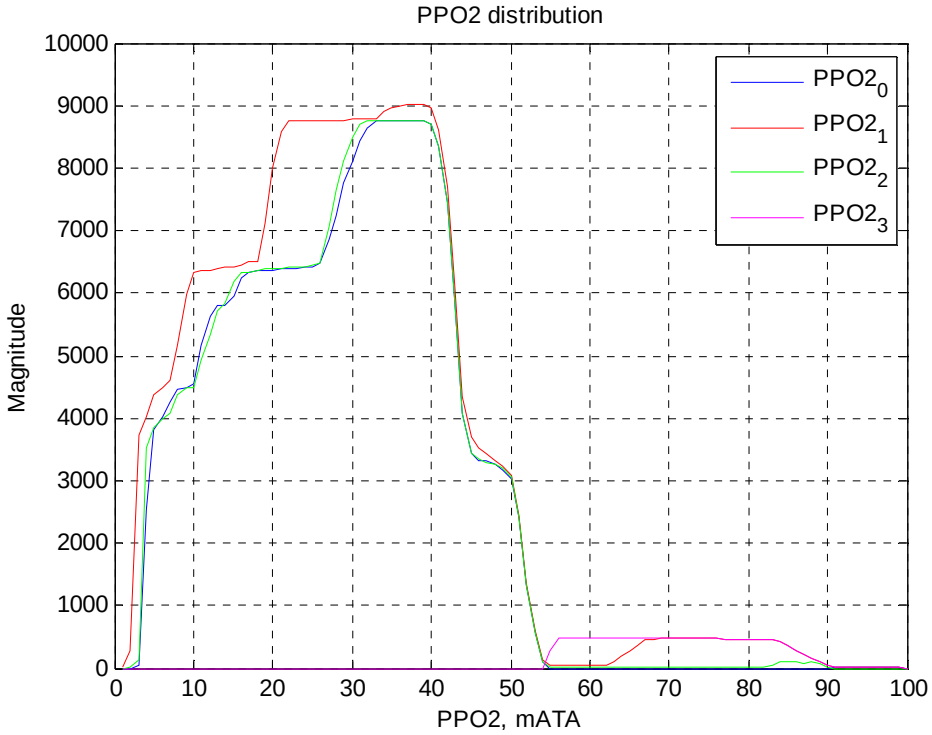


Figure 32. Integral of distributions minus min integral values. Blue and green curves have the closest coincidence in the PPO2 range of 2 .. 90 mATA, as would be expected from visual examination of the test case.

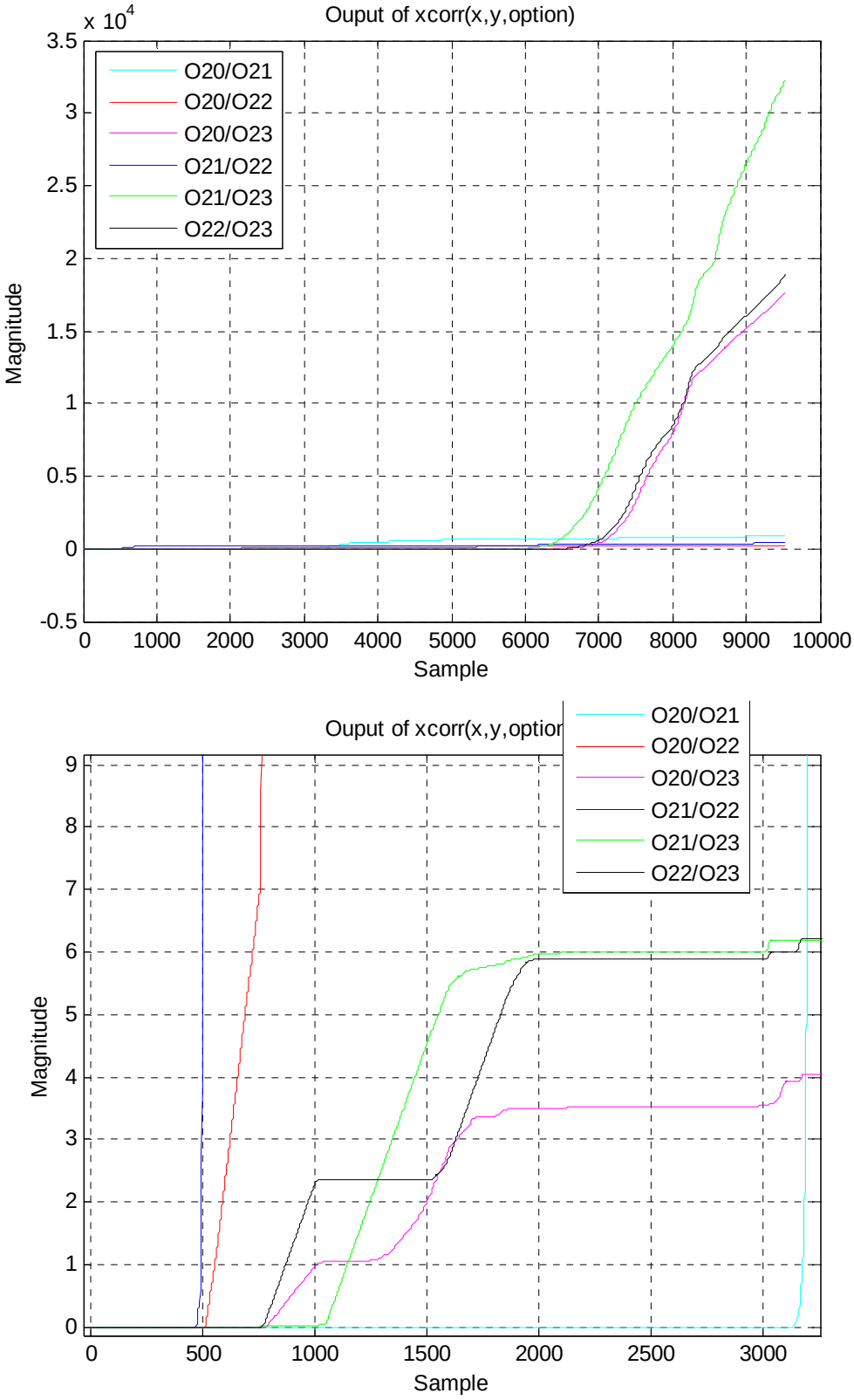


Figure 33. Check on the test data using cross-correlations between the distributions. Note scales.

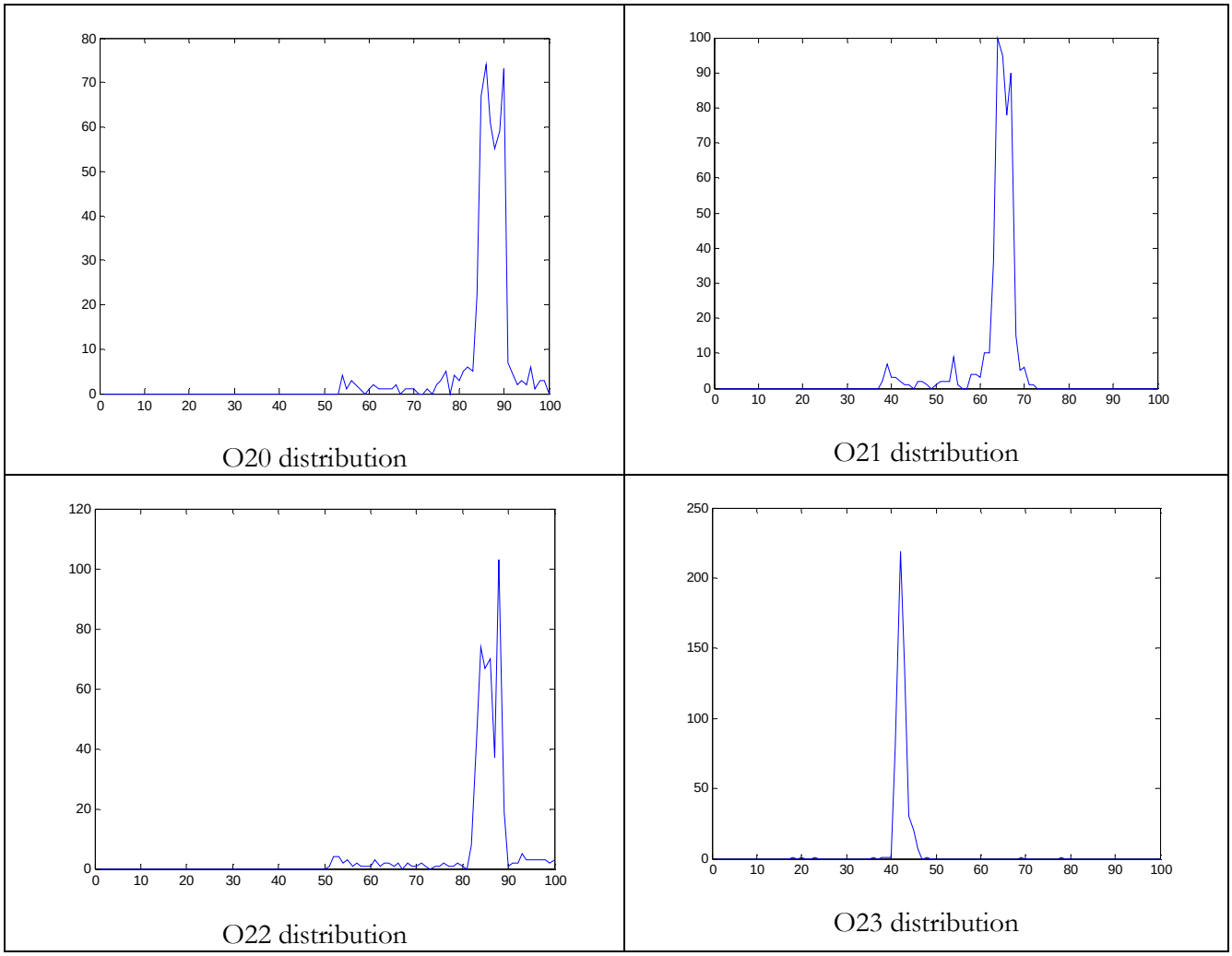
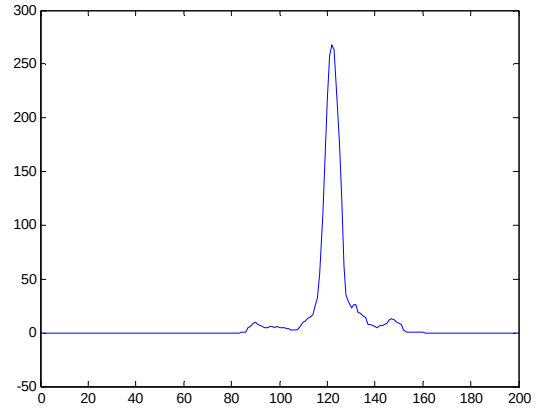
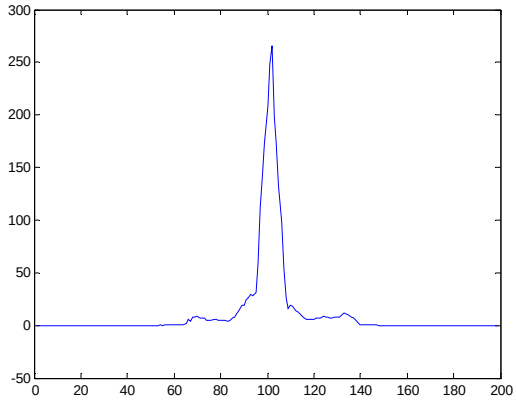


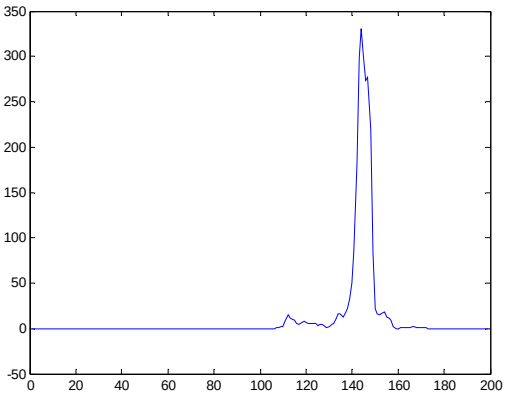
Figure 34. Examination of the distributions of each of the cells.



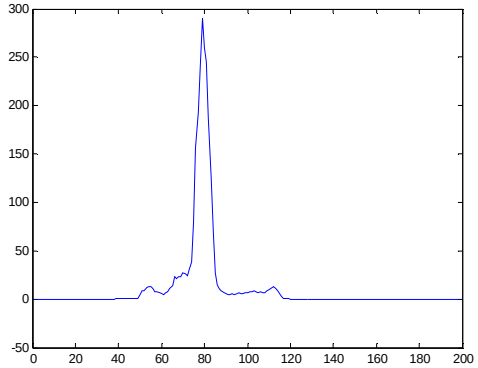
c = xcorr(O20_dist,O21_dist,'biased');



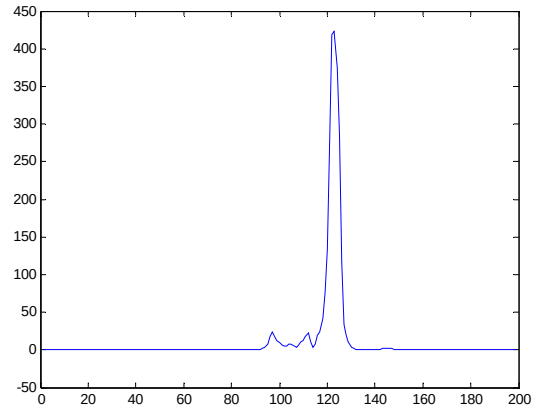
c = xcorr(O20_dist,O22_dist,'biased');



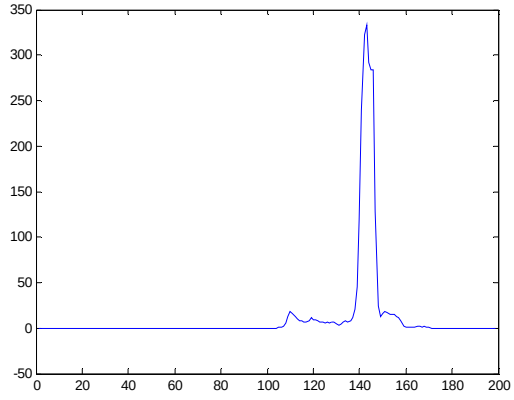
c = xcorr(O20_dist,O23_dist,'biased');



c = xcorr(O21_dist,O22_dist,'biased');



c = xcorr(O21_dist,O23_dist,'biased');



c = xcorr(O22_dist,O23_dist,'biased');

Figure 35. Distribution zoomed to first 500 samples and correlations between the distributions.

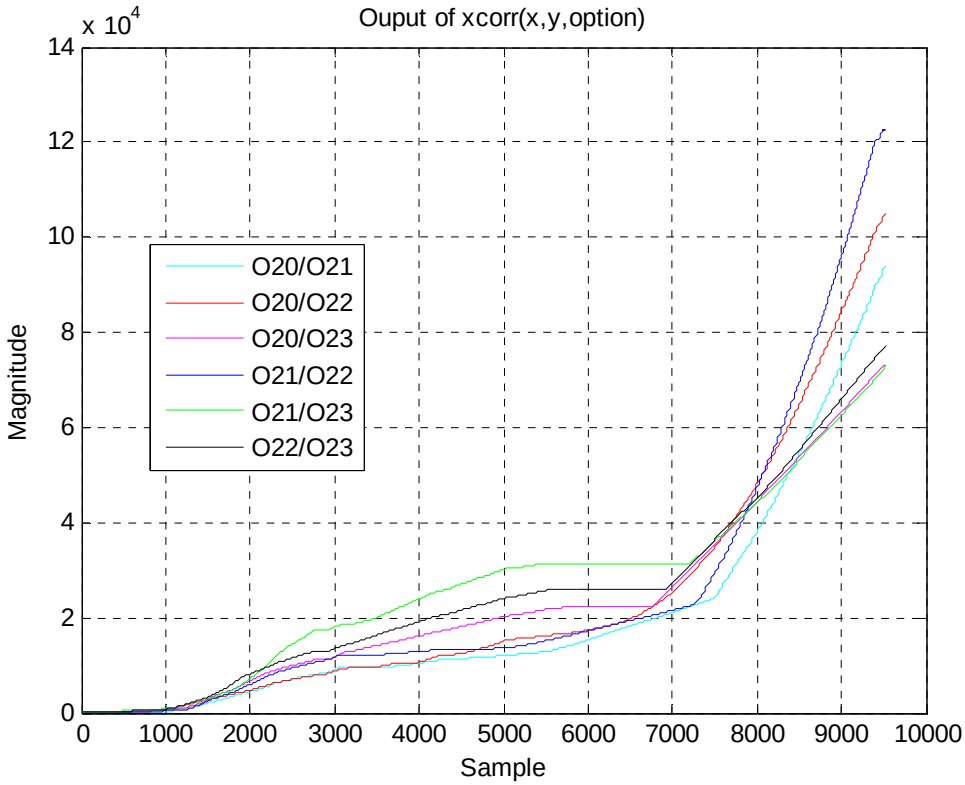


Figure 36. Test data. Maximum correlations against Sample Period, i.e. as a function of the total number of sample periods over which the correlation function is applied.

The checks above confirmed there was no unexpected relationship between the data in this test case. The same checks were applied to each data set of each test case.

6 Other Test Cases

Deep Life has gigabytes of PPO2 data from dives in an SQL-Lite database. Following verification of the above cases, a Monte-Carlo simulation should be applied using dives taken randomly from that test database.

7 Results from Application of Test Cases

All results from applying the test cases listed herein, to the Sensor Fusion Algorithm, form part of the safety case for acceptance of the algorithm.

The requirement for acceptance is that none of these test cases may present a hazard in the diver being exposed to excessively high or low PPO2 levels, as defined within EN 14143:2003. That requirement is checked automatically using a module in SPARK Ada that filters the SFA results to identify exceptions.

8 References

[1] DV_O2_cell_study_E3B_130314.pdf, "Characterisation of Oxygen Cells for Diving Rebreather Applications: Sourcing, Performance, Safety and Reliability. ORIGINATORS: Dr. Bob Davidov, Dr. Alex Deas, Dr. Oleg Zagrebelny, DrVladimir Komarov. Available for download on www.deeplife.co/or_dv.php