National Oceanography Centre, Southampton

Research & Consultancy Report No. 12

Report of the inquiry into the loss of Autosub2 under the Fimbulisen

J E Strutt*

2006

National Oceanography Centre, Southampton
University of Southampton, Waterfront Campus
European Way
Southampton
Hants SO14 3ZH UK

*Author contact details:

Professor J E Strutt
Risk Reliability Division
Boreas Consultants Ltd
Unit 12 Cranfield Innovation Centre
University Way
Cranfield Technology Park
Cranfield, Bedfordshire MK43 0BT
Tel: 44(0) 1234 43 61 60
Email: J.Strutt@boreasconsultants.com

This sheet blank

DOCUMENT DATA SHEET

AUTHOR	*PUBLICATION DATE*
STRUTT, J.E.	2006

TITLE

Report of the Inquiry into the Loss of Autosub2 under the Fimbulisen

REFERENCE

Southampton, UK: National Oceanography Centre, Southampton, 39pp.
(National Oceanography Centre Southampton Research and Consultancy Report, No. 12)
(Unpublished manuscript)

ABSTRACT

The Board of inquiry into the loss of Autosub2 under the Fimbulisen found that the loss was caused by a technical systems failure on the AUV. A comprehensive analysis was made of the technical reasons for the loss. However, because it was not possible to recover the AUV from under the ice shelf for direct examination, it was not possible to identify the actual cause of loss. Consequently an assessment was made of the likelihood of different failure modes causing the loss. The results of this analysis suggest that the loss was equally likely to have come about from an *Abort Command* (AC) as a *Loss of Power* (LP). A root cause analysis was performed which indicated that the source of the failure was most likely to have been a fault introduced during the manufacturing/assembly phase (52%), followed by Maintenance (25%). Design error was considered less likely (14%) while Operations (7%) and External factors (1%) were considered least likely.

This analysis indicates that the greatest benefits to reliability improvements are most likely to come from attention to faults originating in the manufacturing and assembly stage, followed by attention to faults arising from maintenance activities. Due to the large numbers of connections and leakage paths, it is necessary to pay particular attention to the reliability of electrical connectors and harnesses. A high level of quality assurance in manufacture and assembly is required to achieve an acceptable level of system reliability.

While it was accepted that the development team at NOC had adopted sound engineering practices in the development of the AUV and that reliability considerations had informed design decisions, the design team had no formally implemented reliability or technical risk assessment procedures to support design decision making. This was considered to be a major management weakness.

KEYWORDS

AUTOSUB, Autonomous Underwater Vehicles, loss, risk management, reliability, insurance, Antarctic

ISSUING ORGANISATION

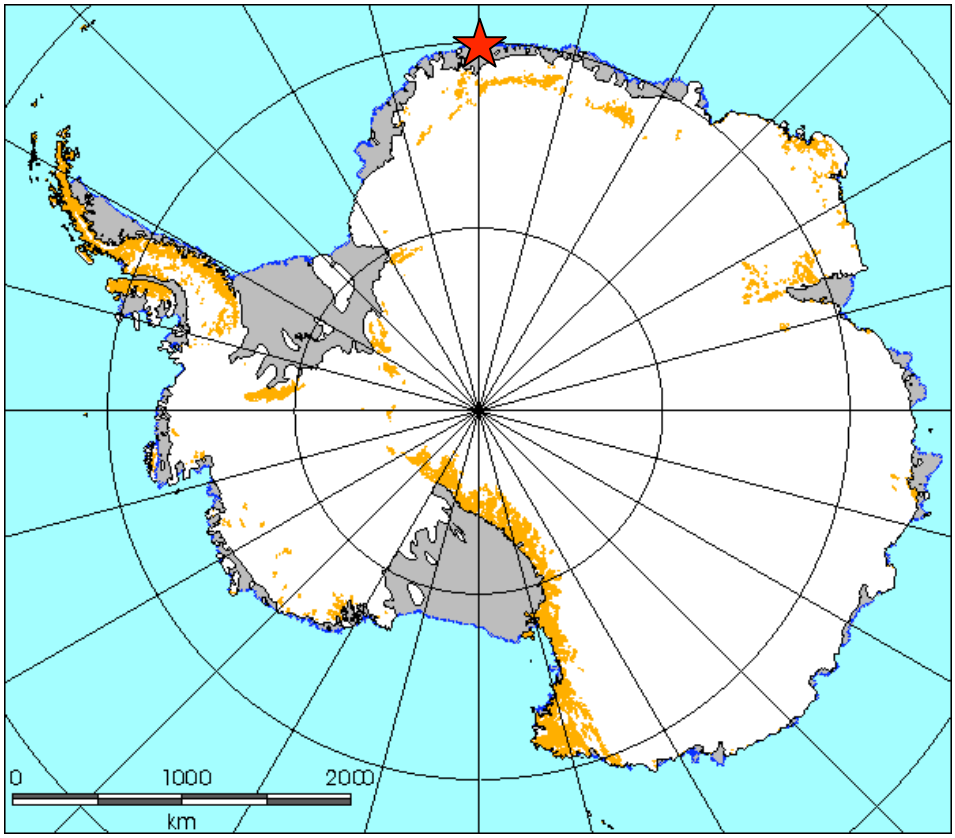
National Oceanography Centre, Southampton
University of Southampton
Waterfront Campus
European Way
Southampton SO14 3ZH
UK

This sheet blank

National Oceanography Centre, Southampton
UNIVERSITY OF SOUTHAMPTON AND NATURAL ENVIRONMENT RESEARCH COUNCIL

Report of the Inquiry into the Loss of Autosub2 under the Fimbulisen

Professor J E Strutt



Summary 7
Scope and Terms of Reference of the Inquiry 9
1 The Loss Event 10
2 Review Method 12
3 Circumstances surrounding the Loss of Autosub2 13
4 Failure Analysis Procedure for the Investigation 15
4.1 Description of the Failure Cause Tree 15
4.2 Event Likelihoods 16
4.3 Identification of the origin of failure 16
5 Analysis of Failure 18
5.1 Level 1 Failure Modes 18
5.2 Level 2 Failure Modes 18
5.3 All Failure Modes 19
5.4 Loss of Power Scenarios (LP) 19
5.5 Abort Command Scenarios (AC) 20
5.6 Joint Event Scenario (JE) 22
5.7 Technical Root Cause Categorisation 22
6 AUV Management Issues 23
6.1 AUV Development History and Method 23
6.2 NOCS AUV Reliability Management practice 24
7 Organisational and Risk Management Issues 27
7.1 Good Risk and Reliability Management Practice 27
7.2 Key Risk and Reliability Processes 29
7.3 Implications for the NERC 30
8 Conclusions 32
9 Recommendations 36
10 References 38
Annex 1 Root Cause Tree 39
Annex 2 AUV Systems Reliability Issues 40
Annex 3 Description of Lon works and CSMA 41
Annex 4 Preliminary Conclusions from Albert J Williams 42

Report of the Inquiry into the Loss of Autosub 2 Under the Fimbulisen

Summary

The Board of inquiry into the loss of Autosub 2 under the Fimbulisen found that the loss was caused by a technical systems failure on the AUV. A comprehensive analysis was made of the technical reasons for the loss. However, because it was not possible to recover the AUV from under the ice shelf for direct examination, it was not possible to identify the actual cause of loss. Consequently an assessment was made of the likelihood of different failure modes causing the loss. The results of this analysis suggest that the loss was equally likely to have come about from an *Abort Command* (AC) as a *Loss of Power* (LP); the most important failure modes causing these events and their likelihoods being:

Cat	N	Failure Mode	Likelihood
LP	1	Open circuit h/w failures	28.5%
AC	2	Network fails for t>20s	23.8%
AC	3	leak sensed for t>20s	20.4%
LP	4	Short circuit h/w failures	9.5%
LP	5	loss of connectivity	7.1%

A root cause analysis was performed which indicated that the source of the failure was most likely to have been a fault introduced during the manufacturing/assembly phase (52%), followed by Maintenance (25%). Design error was considered less likely (14%) while Operations (7%) and External factors (1%) were considered least likely.

This analysis indicates that the greatest benefits to reliability improvements are most likely to come from attention to faults originating in the manufacturing and assembly stage, followed by attention to faults arising from maintenance activities. Due to the large numbers of connections and leakage paths, it is necessary to pay particular attention to the reliability of electrical connectors and harnesses. A high level of quality assurance in manufacture and assembly is required to achieve an acceptable level of system reliability.

While it was accepted that the development team at NOC had adopted sound engineering practices in the development of the AUV and that reliability considerations had informed design decisions, the design team had no formally implemented reliability or technical risk assessment procedures to support design decision making. This was considered to be a major management weakness.

The *Autosub under Ice Programme* is a high risk project. In the event of a failure causing the vehicle to become immobilised it would be difficult if not impossible, to recover. For such projects it is recommended that NERC require design teams to implement good risk management practices aimed at preventing future AUV losses. In particular it is recommended that

1 NERC, or their authorised representatives, should define risk acceptance criteria for future high risk AUV projects.

2 AUV development team should be required, as a condition of contract, to develop capabilities in risk and reliability assessment and management and implement these formally during the development of the AUV and its subsequent operation.

3 The AUV development team should provide evidence of reliability achievement in advance of operation.

4 A number of technical design changes leading to improvements in system reliability have been recommended by the design team. Many of these have already been implemented.

The Review Board

The review Board consisted of the following members

Professor John Strutt	Chair*
Mr David Meldrum	Board Member
Dr Albert J Williams 3rd	Board Member
Mr Simon Corfield	Board Member
Dr Helen Beadman	Board Secretary, NERC
with	
Professor Gwyn Griffiths	Head of Underwater Systems Laboratory, NOCS
Mr Nick Millard	Head of Platforms Group, NOCS
Mr Steve McPhail	Chief AUV Systems Engineer, NOCS

* Formerly Professor of Reliability Engineering and Risk management at Cranfield University and now Head of Risk and Reliability at Boreas Consultants Ltd.

Scope and Terms of Reference of the Inquiry

The following terms of reference were supplied to the Inquiry board:

1. To review the circumstances surrounding the loss of Autosub2 under the Fimbulisen in February 2005 using the available data, documentation and previous results of science and engineering missions.
2. To examine the possible technical reasons for the loss, and, in light of other possible modes of failure, produce a ranked list and suggest mitigating strategies for further minimising risk.
3. Identify possible issues and shortcomings in the organisational aspects including structure, empowerment, authority and resources that might have contributed to the loss.
4. To review the current Autosub risk assessment and risk management procedures and to suggest improvements.
5. To propose options for how NERC might manage risk from the proposed use of future AUVs within science projects.

Report of the Inquiry into the Loss of Autosub2 under the Fimbulisen

1 The Loss Event

On the 16th of February during mission 383 of the 2005 Antarctic campaign, the autonomous underwater vehicle, Autosub2, was stranded a distance of 15km under the Fimbul ice sheet in the Antarctic. Given its location, there is little hope of a successful recovery. An inquiry was initiated by NERC to investigate the possible causes of the loss and to recommend procedures to reduce the risk of similar losses in future science projects. This report is a summary of the work performed during that inquiry.

Autosub2 was developed as the enabling tool to implement the science research programme "*Processes beneath ice shelves: Autosub investigations and implications for the linked ocean-ice climate system*". The programme became known as the *Autosub under Ice Programme*. Funding for this research programme was provided by the Natural Environment Research Council in 2000[1] and was due to complete at the end of year 2005. The focus of the proposal was on the scientific objectives of the missions rather than the AUV technology needed to make the project successful. The first field campaign for the "Autosub under ice" programme began in February 2003 on the RRS James Clark Ross (cruise JR84, PI: Dr Adrian Jenkins) to the Pine Island Bay region of the Antarctic. An Arctic campaign to NE Greenland (JR106) was made in 2004, in two legs, the first to study fast ice thickness (PI: Prof P Wadhams), and the second to study the environment of a fjord (PI: Prof J Dowdeswell). A second Antarctic campaign was made, in February 2005 to the region of the Fimbulisen (JR097, PI: Dr Keith Nicholls).

The Autosub2 vehicle evolved from Autosub1 which had been successfully deployed in previous research programmes and missions. Although the Autosub design objectives were not specifically defined in the proposal, it was recognised that there would need to be a number of technological developments to the "on board" systems of navigation, power, mission-abort and collision avoidance.

Following the upgrade changes, a number of reliability issues were identified during the 2003 Antarctic campaign (JR84). These were subsequently reported[2] at the "Unmanned, Untethered Systems Technology" conference in New Hampshire. Of significance to the current inquiry is the comment that a number of system faults were reported, including:

- O-ring seal leaks
- Connector leaks
- Pulled-out crimp terminals
- Motor fails to start {on one mission & logged as unknown network issue}

A number of other faults which were experienced on missions were traced to intermittent failures of the wet mate connectors which would interrupt the network supply. It was reported that these faults only occurred under pressure (30-50 bar).

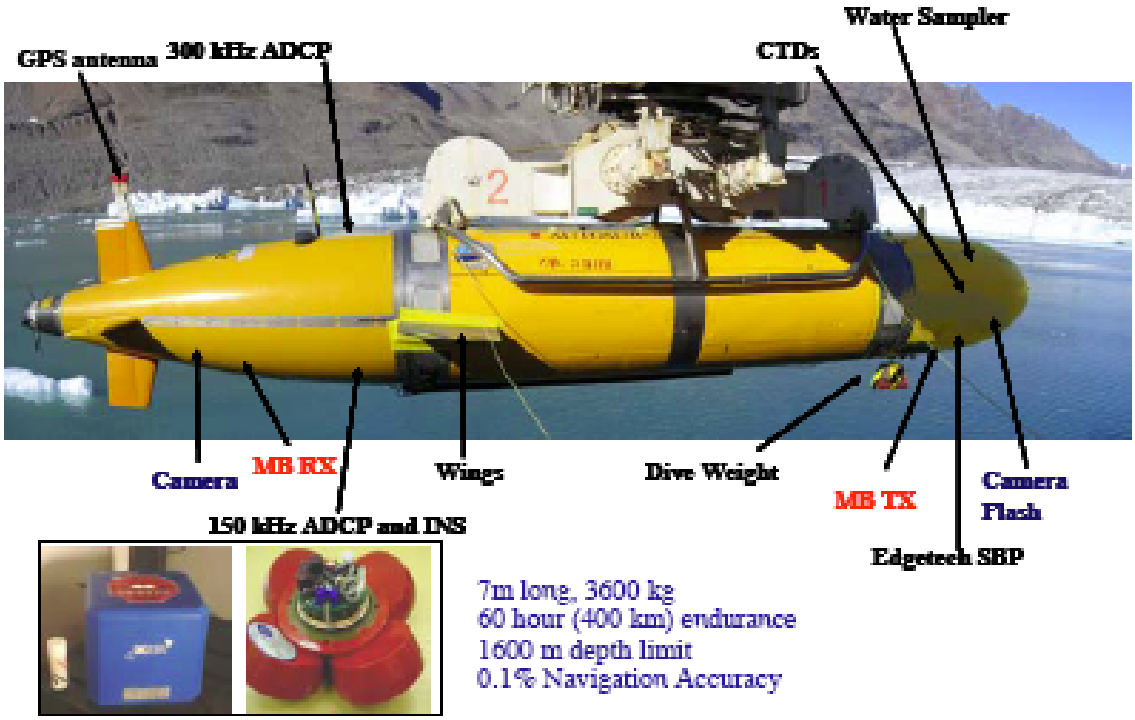


Figure 1: Autosub2

Following the problems experienced on 2003 Antarctic campaign of JR84, the causes of these problems were investigated. Consequently the entire wet harnesses, (based on Impulse IE55 connectors), were replaced using connectors from a different manufacturer (Burton series wet mateable). Following changes to the bulkhead connectors, a quality control check of all the system wiring was carried out.

2 Review Method

The methodology outlined below was used to meet the review objectives.

1) **Understanding the circumstances surrounding the AUV loss**
   Outline presentations were made summarising the circumstances surrounding the loss of the AUV by the design team. This involved:
   a) Outline descriptions of key AUV design features
   b) Description of the AUV development plan and an outline of the organisational structure, design phases, resources and responsibility.
   c) Summary of the circumstances and the design team's explanation of the loss. Discussion of information presented.

2) **Examining the technical causes of the loss**
   Due to time limitations it was not possible to undertake a complete root cause analysis (RCA) of failure or a formal reliability analysis of the AUV systems. However, a simplified RCA method was used to drive the meeting. RCA enabled the review board to identify what, how and why the loss occurred with the aim of identifying specific actions to be taken to prevent loss recurrence. The RCA process involved:
      i) Information/Data review
      ii) Cause–consequence analysis
      iii) Root cause identification
      iv) Recommendations for corrective actions.

   Root causes were addressed both at product and process level:
      v) **Product** level including technical hardware and physical failure mechanisms
      vi) **Process** level including human, management and organisation issues throughout the design-build-operate life cycle.

3) **Reviewing current Autosub2 risk assessment and risk management procedures**
   a) The existing approach to risk assessment and risk management in the project was reviewed. This included a review of :
      i) Tools used to assess risk and reliability
      ii) How these were used to inform decision making in design, construction and operations.

3 Circumstances surrounding the Loss of Autosub2

One under ice mission (mission 382) in the Antarctic 2005 campaign had been successfully completed prior to mission 383. Mission 383 was similar to 382 in terms of overall distance and start position. One major difference was that the profile for 383 was a yo-yo profile as shown in figure 2.

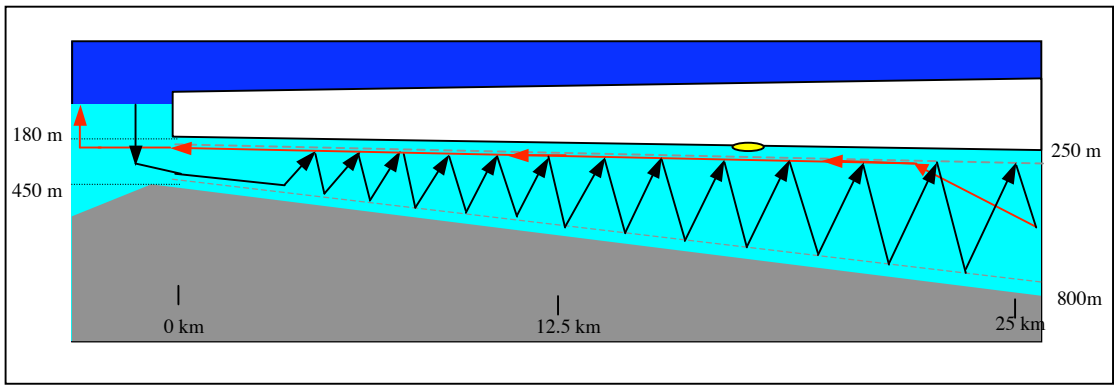


Figure 2: profile for mission 383 under the Fimbulisen.

An initial analysis of the circumstances and description of the known facts surrounding the loss of the AUV was carried out by Mr S McPhail of the National Oceanography Centre (NOC)[4]. The sequence of events was reported as follows (this is a brief summary)

Date: 16th February 2005

07.33 AUV launched and dived using dive weights: no abnormality noted
AUV circled around the start way point: awaiting acoustic command to start

07.43 Acoustic telemetry from the vehicle received. All nominal.

07.44 Transmission from Emergency beacon received (at the normal (non emergency) rate of one transmission every 10 min.

07.45 Acoustic telemetry from the vehicle received. All nominal.

07.48 Command signal sent to start mission: Acknowledged by Autosub: all systems normal

08.28 Emergency beacon listening transducer pulled inboard
Vehicle was 3km under the ice shelf when monitoring ceased
No monitoring for next 5 hours

13.33 Listening beacon activated:
AUV now transmitting at 1 per min indicating distress[†]
Position located as S: 70 10.25, W:0110.64
Distance 17.5km from start position
Location was 194m south west of its intended track

15.54 Start transmitting homing signal at full power

16.16 Stopped transmitting

16.17 Triangulation showed no change in range. Vehicle appears to be stranded.

Date: 21st February 2005

[†] The emergency beacon is a 4.5 kHz acoustic transmitter. When an abort event occurs on the AUV the acoustic projector array is dropped on a 15m cable under the Autosub and it begins to transmit a chirp at a frequency of 1 per minute

The Ship returned to the ice shelf front 5 days later. Triangulation showed that Autosub had moved less than 250m. This displacement is within the error bound of the triangulation measurement system and so it was concluded that Autosub2 had not moved from the position noted on the 16th of February.

What is known then is that Autosub2 was immobile and that the beacon was down and chirping at a frequency of 1 per minute. The next task was to assess how that state could have arisen.

4 Failure Analysis Procedure for the Investigation

Because the AUV failed under the ice shelf and cannot be retrieved, it has not been possible to directly inspect the vehicle or its component hardware to ascertain the actual cause of failure as would be the normal procedure in failure investigation. The failure analysis, therefore, was based on an assessment of *cause probability*. To this end, the failure analysis was carried out using an event tree method from which it was possible to assess possible causes of the Autosub loss. The fault condition assumed for the analysis was based on the known facts, namely that the A*UV was immobile and that the beacon was down and transmitting with a chirp frequency of 1 per min.* The possible causes of the failure were then analysed in turn. In the meeting the tree was mapped on a flip chart, using the board members as experts to make judgements on the likelihood of particular causes of failure. The results of this exercise were subsequently transferred into Microsoft XL with the Precision Tree add-in[‡]. In a later meeting the failure logic and associated likelihoods were rechecked with the designers S McPhail and N Millard. Some minor modifications to the logic were made at that time and further root-cause categories were added to support analysis.

4.1 Description of the Failure Cause Tree

The overall cause tree structure is shown in annex 1. The following describes how the tree was built and how to interpret the figures. A complete description of the tree logic is provided in section 5 “Analysis of Failure”.

The tree starts with the event “AUV loss” on the left hand side of the diagram. Possible causes of the loss event are shown to the right of that event. The red round symbols represent chance events. Thus, the start of the tree is the loss event itself. The review board was then asked; given the loss what could have been the cause of the loss? Four failure routes were identified namely: an *abort event*, an event involving a *loss of power for a time greater than 20ms* and a *joint event*. The team then provided Likelihoods that each was the true cause of loss were then assigned to each of these paths. The joint event failure mode (5%) was considered to be quite unlikely compared with Abort and loss of power which were considered equally likely (47.5% each).

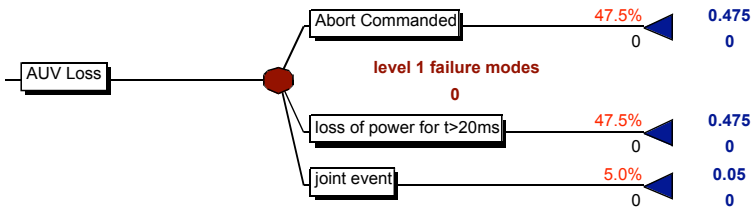


Figure 3: Level 1 failures in the cause tree

Each event was then further broken down into its possible causes and likelihoods assigned to each of these. For example, the event Abort commanded was analysed to have the 5 possible causes shown in figure 4; (i) network failure for longer than 20s, (ii) leak sensed for longer than 20s, (iii) mission time out, (iv) dive time out and (v) depth exceeded. Of these, the network failure for t > 20s was considered most likely (50%) of the failure modes and the sensing of a leak was next most likely (43%). The events mission time out and dive time out were considered very unlikely but possible and it was felt that there was a 5% chance of the depth exceedance. Precision tree automatically calculates the probability of AUV loss caused by a network failure via an abort command as 0.2375.

[‡] Precision tree this is a conventional decision analysis tool marketed with @ Risk by Palisade Corporation

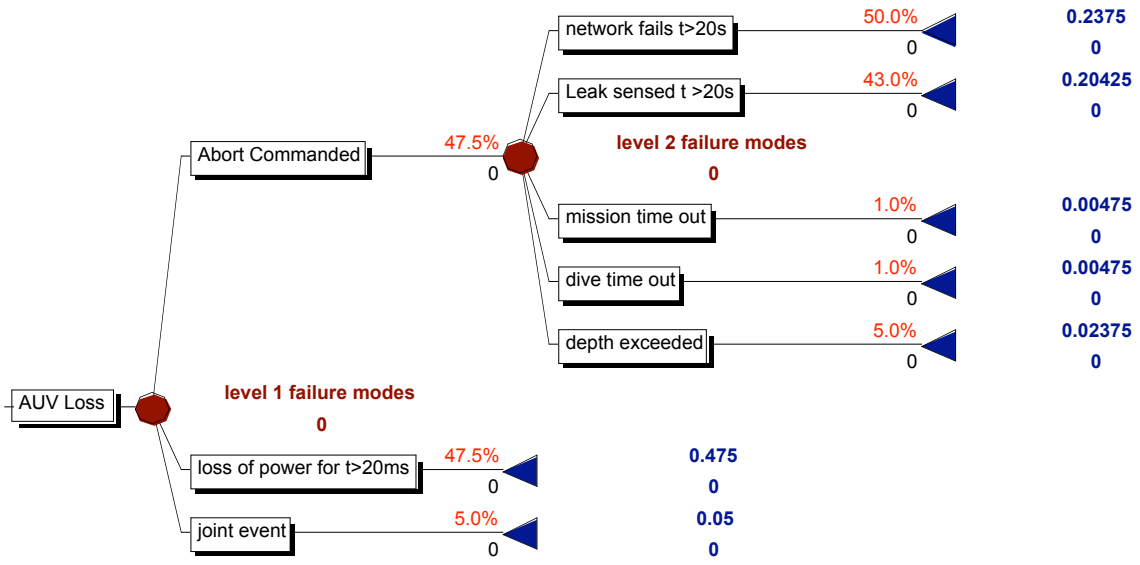


Figure 4: Level 1 and Level 2 failures

This procedure continued through all the potential failure modes down to a level below which it was not considered useful to go further.

4.2 Event Likelihoods

The figures in the trees are conditional probabilities or likelihoods associated with each event. They represent the combined beliefs of the Inquiry board. However, the greatest weight was given to the original equipment designers beliefs. Had "hard" failure mode data been available this could have been used in place of the subjective data. However, hard data was not available to support this analysis.

While it is easy to criticise the use of subjective data, it was felt to be useful as an input to interpretation. This procedure enabled an overall judgement to be made on the most likely failure modes. The results of this analysis are described in section 5 below.

4.3 Identification of the origin of failure

The origin of the failure must have occurred as a result of an internal fault/failure or as a result of an external factor. Internal faults must have originated at sometime during the life cycle of the AUV, i.e. in design, manufacture and assembly, maintenance or during operation of the vehicle. In order to facilitate preventive and corrective actions in the future it was felt important to identify the origin of the loss. To this end 5 technical root cause categories (TRCs) were considered, namely; (i) external environment (the most likely being a mechanical impact), (ii) design error, (iii) manufacturing and assembly error, (iv) maintenance error and (v) operator error. The event tree model was used to support this analysis by terminating all the braches of the tree by these 5 TRC factors and assigning a likelihood that the fault was caused by one of the TRC factors.

Table 1 provides description of the meaning of the root cause. The approach taken here was to indicate where in the life cycle of the vehicle the error might have occurred. In this study the term assembly refers to manual assembly of parts into the vehicle prior to mission. Manufacture refers to bought in parts created by an external manufacturer. It was difficult in some cases to treat these as independent root causes and so they have been combined.

	Cause category	Interpretation
1	Design	A failure event which is caused by a design error. For example specification of the wrong component in a circuit.
2	Manufacture/assembly	A failure event caused by a manufacturing error. For example a dry joint in a machine soldered connection or a failure event triggered by an assembly error. For example forcing a component to fit in a limited space such that the component is overstressed or providing too little or too much torque on a threaded fitting during assembly.
3	Maintenance	A failure event caused by a maintenance error such as an incorrectly replaced part or a incorrectly adjusted torque on a connector
4	Operation	A failure event caused by the incorrect operation of the vehicle. For example incorrect instructions from the Mother ship.
5	External	An event caused by some external, environmental factor such as complex terrain

Table 1: Meaning of the technical root causes

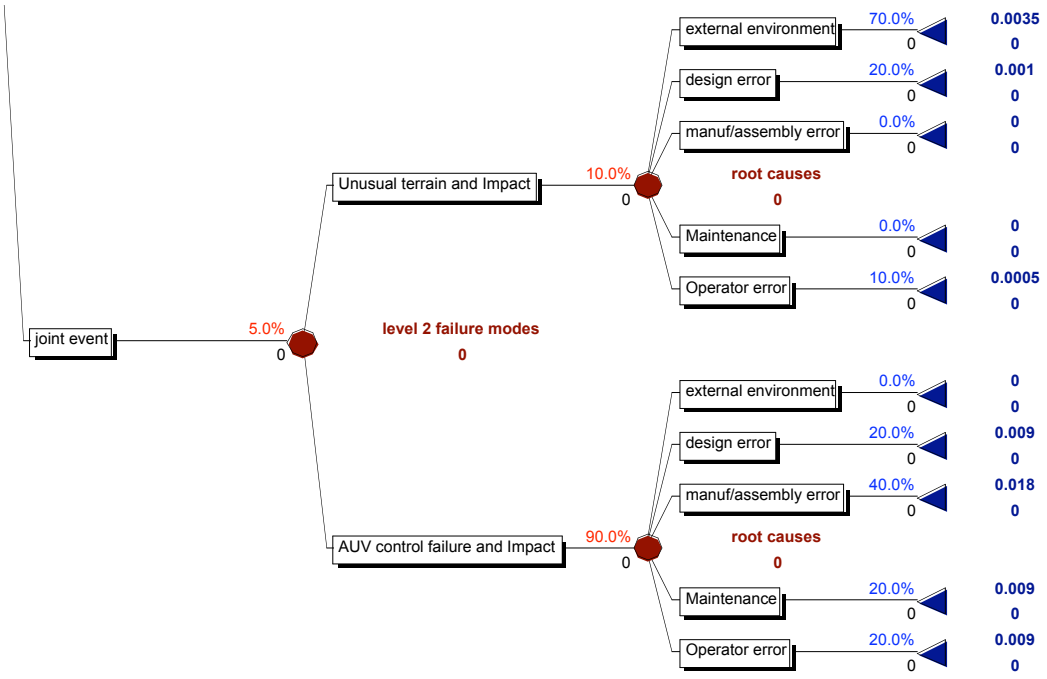


Figure 5: Technical Root causes of the "joint events" Unusual terrain and impact and AUV control failure and impact

Figure 5 provides one example of the technical root-cause categories added to one of the tree terminations and the assigned cause likelihood. This same approach was applied to all the scenarios investigated by the team, each branch of the tree terminating with the 5 root causes. At the end of the trees all the TRCs were collated to generate an overall assessment of the cause likelihood within the 5 cause categories.

5 Analysis of Failure

This section describes the analysis of failure carried out during the review. In this section of the report, some of the material in this section has been copied and edited from the report prepared by Steve McPhail[4] in March 2005.

5.1 Level 1 Failure Modes

The condition of the AUV at the time the loss was identified was as follows:

1. The distress beacon had been activated and was sending out a distress signal
2. The vessel was immobile. There had been no movement for 5 days.

The AUV was believed to be floating because there was clean signal from the AUV at the ship. The review team concluded that there were 3 possible scenarios or explanations for this condition, namely; an *Abort Command* (AC), a *Loss of Power for a time t>20ms* (LP), or a *Joint Event* (JE). These are shown in the table below together with review board assessment of likelihoods.

Cat	Failure Mode	Likelihood
AC	Abort Commanded	0.475
LP	Loss of power for t > 20ms	0.475
JE	Joint event	0.050
	TOTAL	1

Table 3: Level 1 failure modes

The failure modes are represented as uncertain options in the tree (appendix 1) as the first three branches from the top event "AUV loss". A description of these three scenarios is outlined below. As the tree was drawn, at each stage, the review team considered the likelihood that this possible cause was the true (actual) cause of the failure. There were 3 distinct modes by which the failure could have occurred; an event may have occurred which triggered an abort command (AC), there could have been a loss of power for a time (LP), or there could have been a simultaneous event (JE) in which the vessel was prevented from returning home and at the same time the distress beacon had been activated.

At this level in the cause hierarchy the experts could not really distinguish between the loss being caused by an Abort command (AC) or a loss of power (LP). However, the board was very clear that the joint event scenario (likelihood 0.05) was far less likely.

5.2 Level 2 Failure Modes

The analysis then moved to the next level of analysis; level 2. The Failure modes for Abort commanded, Loss of power and Joint event at level 2 are:

Cat	N	Failure Mode	Likelihood	
LP	1	Open circuit h/w failures	0.285	
LP	2	short circuit h/w failures	0.095	
LP	3	loss of connectivity	0.071	
LP	4	battery exhausted	0.024	0.475
JE	5	AUV control failure and Impact together	0.045	
JE	6	unusual terrain impact	0.005	0.050
AC	7	Network fails for t>20ms	0.238	
AC	8	leak sensed for t>20ms	0.204	
AC	9	depth exceeded	0.024	
AC	10	Mission time out	0.005	
AC	11	dive time out	0.005	0.475
		TOTAL	1.000	

Table 4 Level 2 Failure Modes

5.3 All Failure Modes

At the deepest level of analysis in this study the complete list of failure modes were identified as those listed in table5 below. Sixteen failure modes were found to be linked to loss of power. A further nineteen failure modes were found to linked to the Abort Command and finally two modes were linked to the Joint event scenario. These are discussed further below.

Cat	N	Failure Mode	Likelihood	
LP	1	NetX in dry domain fails	0.086	
LP	2	NetY in dry damain fails	0.048	
LP	3	NetY in wet domain fails	0.048	
LP	4	DGO connector failure	0.046	
LP	5	harness joint failure	0.041	
LP	6	Endcap seal failure	0.038	
LP	7	Burton connector failure	0.031	
LP	8	bulkhead connection (netX) fails	0.029	
LP	9	harness failure (netX wet)	0.029	
LP	10	depth exceeded	0.024	
LP	11	Leakage thru bonding on transition ring	0.015	
LP	12	Connector plug failure	0.015	
LP	13	Sensor failure	0.010	
LP	14	Internal Condensation	0.008	
LP	15	Mission time out	0.005	
LP	16	dive time out	0.005	0.475
AC	17	pcb wiring failure	0.048	
AC	18	current sensing resistor failure	0.048	
AC	19	Inrush current protector	0.048	
AC	20	dc-dc converter (fused)	0.048	
AC	21	magswitch failure	0.048	
AC	22	main power switch failure	0.048	
AC	23	motor controller fails	0.038	
AC	24	short circuit on harness	0.038	
AC	25	fuse pot fails	0.021	
AC	26	Net X fails in dry domain	0.017	
AC	27	Short on wires in maintenance	0.014	
AC	28	bulkhead connection (netX) fails	0.013	
AC	29	harness failure (netX wet)	0.013	
AC	30	battery exhausted thru high currernt demand	0.012	
AC	31	fuse and diode fail	0.007	
AC	32	calculation error in battery life	0.005	
AC	33	dc-dc converter failure	0.005	
AC	34	harness connector fails in dry domain (low resistance path)	0.004	
AC	35	harness connector fails in wet domain (low resistance path)	0.004	0.475
JE	36	AUV control failure and Impact together	0.045	
JE	37	unusual terrain impact	0.005	0.050
		TOTAL	1	1

Table 5: All Failure Modes

5.4 Loss of Power Scenarios (LP)

As stated in the level 1 analysis, one way that the AUV could have been lost is through a simple loss of power. Due to the way that the system has been designed, the loss would only need to occur for a short duration, i.e. greater than 20ms for the system to stop. Four distinct failure mechanisms were thought to be possible:

1. Battery exhaustion P = 0.05
2. Loss of connectivity in the power circuit P = 0.15
3. Short Circuit hardware failure P = 0.20
4. Open Circuit hardware failure P = 0.60

Batter Exhaustion: One possibility for loss of power is that the battery might have been low. This path was estimated to have a small chance (5%) of occurrence. But if it had occurred it could have caused by 3 causes, namely; calculation error (20%), an unusually high current demand (50%) or a low resistance path causing a current drain on the battery (30%). Section 3 of reference 4 provides a discussion on the current demand and battery characteristics.

Loss of Connectivity in Power circuit: A loss of connectivity could have occurred in the power circuits. Three possible routes for this mechanism were addressed. There are various fuse and diode components in the batteries that could have failed (10%) or a fuse pot could have failed (30%). However, the most likely cause of loss of connectivity would have been a failure of Network X (60%). Network failures, both Net X and Net Y are implicated in other failure modes.

Short Circuit hardware failure: A short circuit failure could occur by various mechanisms. The following modes were considered; a motor controller failure (40%), a short circuit on the harness (40%), a short created during maintenance (15%) and a failure of the dc-dc converter (5%).

Open Circuit hardware failure: An open circuit failure was considered the most likely mechanism for loss of power. There are plenty of opportunities for this type of failure. The following modes were considered; failure of printed circuit board (pcb) wiring (10%), a blown current sensor (10%), in-rush current protector failure (10%), the dc-dc converter could have fused (10%) and the "magnetic" switch (10%) or main power switches could have failed (10%). The most likely source of this failure, however, was failure of the Fuse supplying the dc. - dc converter which was considered four times more likely than the other failure modes (40%).

5.5 Abort Command Scenarios (AC)

The system could initiate an abort given one or more of the following conditions.

1. Network fails for t>20s
2. leak sensed for t>20s
3. depth exceeded
4. Mission time out
5. dive time out

Network Failures: A network failure on both Net X and Net Y could have resulted in a command to abort. The latest configuration file for Release B.2 (abort node) showed the abort node to be triggered by a failure to communicate with the Depth Control system over the network (ncS2RespNetDownX) a network failure involving loss of communication with the Seapam acoustic telemetry system (ncS2RespNetDownY), a power system fault, mission timeout and dive timeout. The hold off time for these events is 20 seconds and had been at this setting since the JR84 Pine Island campaign of 2003.

The testing of the communication link with the SeaPam (housed in the front of the vehicle) and the Depth control node (housed in the motor enclosure), involves deliberately testing the integrity of the network from the front to the tail of the vehicle and this involves connections through 6 wet mateable connectors. The network is checked at a rate of 2 attempts per second and if no reply is heard for a period of 40 contiguous attempts to communicate with the test nodes over the network, then the Abort command is triggered. At the network level, there is no hierarchical control. It is a peer to peer, asynchronous, multiple access network. Hence the network as a whole cannot be restarted. Loss of the network communications for such a long period is considered as an irrecoverable fault. However, if the application code in a particular node hangs up (e.g. in the SeaPam or DepthControl nodes), then a watchdog timer will activate after 0.6 seconds, resetting the node.

Following problems with wet mateable underwater connectors, during the Antarctic campaign of JR84 (Pine Island), all the Impulse underwater connectors in Autosub were replaced with a different manufacturer's model (Burtons type 5501-2008), of different design. No problems with network loss had been experienced since then, with tests carried out at up to 1500m water depth, well in excess of those in mission 383.

The Burton connectors had recognised problems (see also annex 4); once pressured and then fully depressurised, the locking ring for the connectors could become loose, presumably due to compression of the rubber parts when under pressure. There is nearly always some degree of hysteresis in the mechanical behaviour of rubbers such that they do not fully expand again on depressurisation. This is a significant issue, because the connectors have a single face seal, which depends upon pressure applied by the locking ring for the low pressure water tightness. It is also significant in that the AUV trajectory in mission 383 involved a saw tooth profile; the seals will therefore have been through many hysteresis cycles. The Burton connectors have been a source of concern for the AUV team for some time and as a result had initiated a series of pressure cycle tests on the harnesses (more than 100 cycles between 0 to 650 bar and in later tests this pressure range was increased 1000bar). During these tests the connectors did show some increase in resistance during a pressure cycle, however, throughout these tests there was no evidence of water leakage through the connector seals.

The effects of hysteresis on seal integrity have not been fully evaluated but the consequences of a loss of seal integrity are quite clear. A leak of water into the pins could disrupt the network or power connections (network, 24 volt, and 48 volt bus are all carried on the these connectors), sufficiently to cause an abort, either due to network failure, or power failure (although the network would be more easily disrupted than the power system).

The AUV design team had initiated procedures to check the tightness of all wet connectors, prior to a deployment of Autosub and this was carried out prior to Mission 383. No network connectors were re-seated between Mission 382 and Mission 383. The data for Mission 382 indicated no outages to the network exceeding 2 samples (4 seconds).

Leak Sensor: A leak in one of the main pressure cases or a failed sensor could cause abort of the mission. The monitoring of the leak sensors, and of the control logic which determines which power related (or leak) condition can cause abort is handled by the Power Node (which is located in the central main tube). The configuration variable "ncAlarmMask" determines which events could cause the abort from one of over-temperature, battery under-voltage or leak. The latest configuration file for the power node showed that the configuration variable ncAlarmMask was set to Hexadecimal 0200. This masks out all except the leak indication.

Within each of the 7 main pressure cases a leak sensor runs the entire length of the tubes. These sensors are wired in parallel, so that a leak in any of the tubes can be detected. The leak sensors also have known value resistors connected in parallel, so that if a leak sensor becomes disconnected, this is also detected. This is checked as part of the standard pre-mission check but its failure does not cause an abort.

Four of the pressure vessels are regularly opened for main battery change. One pressure case (holding the EM2000) was opened prior to operations on JR97, to replace a faulty memory card on the EM2000 system. No pressure cases were opened following the commencement of JR97 trials (over two separate days), mission 382 and the final mission.

No problems were discovered with the leak sensors during the summer 2004 campaigns for which the water temperatures were similar, and the maximum depth (900 m) exceeded the maximum expected depth for mission 383. In fact the leak sensors have never indicated a leak in the main pressure case, and no leaks have ever been found in pressure vessels with leak sensors. This suggests no failure of leak detectors to indicate leaks.

The fact that the Autosub appeared to be still floating 1 week after the incident, suggests that there has not been a major pressure case leak, although floatation would not necessarily indicate no leakage at all.

Depth exceedance: there is a depth limit with an abort threshold of 1700 m. This was set correctly for mission 383, from evidence in the mission configuration file. Only a faulty depth sensor reading continuously for more than 20 seconds reading greater than 1700m could cause this trigger. The depth sensor has never in the past shown such behaviour. Previous pressure sensor data records have never revealed glitches of any kind.

Mission and dive time out: There is a dive time limit, distinct from the mission time. The settings for Mission Abort Time (time since start of mission to abort), to Dive time (time since Dived to abort), and Maximum Depth, are mission dependent, and as such are downloaded as part of the mission configuration procedure (see check list). The mission history download file confirms that these have been successfully downloaded.

Checks performed on the mission history files revealed no configuration errors. The only other reason for the timers to have been set improperly would be a software error within the down-loader, or software error within the Autosub nodes. This seems unlikely as the times and abort setting were identical to those for the Mission 382, and no such occurrence has been seen in the past.

5.6 Joint Event Scenario (JE)

In this scenario an event, such as an impact, would have had to occur with sufficient force to cause the beacon to drop and independently of this event, the AUV would have to have entered some unusual domain such as an ice cave or a crevice from which it could not escape. The likelihood of this event was considered small (5%) relative to the other two contender scenarios. Two sources of evidence were sited; the fact that there was a clear signal meant that it was less likely to be trapped in an ice cave or crevice, the fact that previous impacts that the AUV had experienced had not triggered the beacon to fall.

5.7 Technical Root Cause Categorisation

Failures were grouped into five technical root cause categories, namely: Design, Manufacture/Assembly, Maintenance, Operation and External as described in section 4.3.

The results of this exercise are shown in table 6. This clearly shows which project phase was considered the most important contributor to the loss. The review team believes that the cause of the loss is *unlikely* to be due to external (environmental) causes. The probability that external factors were the technical root cause of failure was assessed as 0.01(1%) *or* to Operational causes (P=7%). Design was considered a possible cause but this possibility was considered less likely than an error in maintenance or assembly. The most likely cause of failure was thought therefore to be through an error made in manufacturing or assembly (52%). This is consistent with the most likely failure modes being associated with network failures. This result indicates where risk reduction actions should be prioritised.

1	Design	0.141
2	Manuf/Assembly	0.521
3	Maintenance	0.255
4	Operation	0.073
5	External	0.010

Table 6 Cause Categorisation

6 AUV Management Issues

The National Oceanography Centre's AUV team has involved the following staff since 1991.

Nick Millard (Project manager)	1995 to present
Peter Stevenson (Chief Mechanical engineer)	1991 to present
Andy Web (Mech. engineer)	1993 to present
Kevin Saw / Mark Squires	2000 to present
Steve McPhail (Chief Systems engineer)	1991 to present
James Perrett (Electronics & SW)	1991 to present
Miles Peabody (Electronics & SW)	1996 to present
James Riggs (Electronics & SW)	2001 to 2004
Dave White (Electronics & SW)	2004 to present

6.1 AUV Development History and Method

The design philosophy of the AUV has evolved over the last 15 years. A key issue being the change from a centralisation control system to a distributed system. In the early 1990s it was recognised that a formal structured method would be needed for software and systems development. At that time various approaches, which were new at that time, were implemented, including; DFDS (Data Flow Diagrams), SCs (Structure Charts), STDs (State Transition Diagrams). In the early stages of development the NOCS team planned to utilise a conventional centralised system involving 68020 processors with a real time operating system (RTOS). However, a number of critical design issues, related to primitive inter-task communications and multi-tasking problems were soon recognised and at the same time, the team were concerned with technical hardware issues related to the physical integration of the various on-board systems; connectors and wiring were particularly singled out as issues to address. At about the same time, the NOCS team heard that a group at Florida Atlantic University (FAU) were using a novel network system, called Lonworks (see Annex 3 for brief description of Lonworks) for system integration purposes on an AUV with centralised control.

The team originally planned to use this as an aid to systems integration. However, it was soon realised that the same network system could be used as the entire basis of a truly distributed system.

It was recognised by the design team that "*system complexity is the enemy of reliability*". A fully distributed system held a number of advantages at hardware and project management level. These were understood as follows:

Hardware: At the hardware level, a distributed system simplifies the system by dividing the system into a network with nodes in which no node was overly complicated, *a divide and rule strategy,* as the NOC team put it.

Project Management: each "node" on the network can be assigned to an individual engineer, who becomes responsible for its development lifecycle. This facilitates sub-system development, testing and straightforward integration at the physical level.

Use of Lon Works: The NOC team noted a number of advantages to using LonWorks. These included:

- Physical implementation was through simple twisted pairs, which are galvanically isolated.
- An implementation of CSMA (see Annex 2 for brief description) which is optimised for real time control
- The operating system, programming language, network and hardware are all integrated.
- Safer in that many problems are detected by the compiler and it employs a watchdog system
- A simple yet safe scheduling mechanism
- Simple to implement networked data communications. In conventional system a high percentage of code is associated with data communications.

Training: In the early days of the AUV project, the NOC team required some education and training in a number of areas including:

- Systems analysis and Systems Design (SA/SD) methods (course)
- Control engineering (gained through an Open University MSc Module)
- Software Engineering (through an Open University Module)
- MSc in Telematics (coms, signal processing, programming, Formal methods. ADA.)
- Real Time Operating Systems (RTOS) training in VRTX32
- Advanced Programming in C
- Programming in Neuron C (LonWorks).
- MSc in Digital Signal Processing

Hardware Quality Control: The NOC team do all of their own internal (dry) wiring. The external harness is contracted out. A quality control check is performed following any major changes to the electronics "chassis", including:

- Mechanical (anti- vibration, shake-proof washers or lock-tight applied to fixings, correctly torqued bulkhead connectors)
- Electrical isolation tests
- Basic electrical continuity test for the network and power circuits
- Wiring looms (protection, anti-vibration, checks for continuity and short circuits)
- Connectors (pull test, crimps ok, locked, strain relief)

6.2 NOCS AUV Reliability Management practice

The AUV development team listed their main activities as:

a) Design of the AUV i.e. the package delivery system
b) Integration and assembly of bought-in parts for the deployment and control of the vehicle and
c) Integration of purpose of built science packages from the various research teams.
d) Field Operation of the vehicle during campaigns
e) Maintenance of the vehicle offshore during field campaigns (between missions)
f) Maintenance onshore between campaigns.
g) System upgrades which involve iteration through (a) to (f) above.

The AUV team are responsible for the complete life cycle of the AUV package delivery system and although they are not responsible for the design of the science packages installed on the AUV, they are responsible for their integration into the vehicle. The following is a brief review of the reliability implications.

Design: The overall delivery system design architecture and configuration are completely under the control of the design team and as a consequence the reliability of the vehicle system is under design control. While it is clear that product reliability considerations have informed design decision making, there have been no formal assessments of system reliability. This is considered to be an important omission in the AUV team's current management practice.

Bought-in manufactured items: A number of important failure modes are directly associated with bought-in manufactured items such as nodes, wet connectors and harness. The reliability of these components is not under the control of the AUV design team and thus represents a significant risk. If there were a choice of supplier, the design team could, in principle, influence system reliability by selecting the more reliable components. Where the manufactured components are one–off, or from limited population, historical failure rate data on components is unlikely to be available. Where the manufactured components are produced in volume, e.g. electronic components, suppliers can usually provide relevant historical failure rate data, but for many components, the lack of relevant reliability data limits the designer's ability to select more reliable components.

Achieving an acceptable level of reliability of bought in items in a research programme such as this is acknowledged to be difficult. One of the problems faced by the AUV team, or indeed any manufacturer purchasing small quantities of product, is their limited power to influence suppliers to deliver higher reliability components.

Where there are alternative suppliers of bought in items and where the product is produced in small volumes, it may be practicable to look into the capability of the supplier to deliver a reliable product and then select the supplier with the better capability. Methods are available to assess reliability capability maturity of suppliers. If there is only one supplier then, there is little that can be done apart from funding the supplier to develop higher reliability products, which may not be financially viable for NERC funded projects.

Integration of bought-in items and system assembly: The integration and assembly of the various components and packages is clearly under the control of the AUV development team. Many of the joints and connections are made up in the labs at Southampton. This is a manual task and the assembler's skills are crucial to reliability achievement.

A simple calculation of the reliability of a soldering task is made below to illustrate the potential scale of the problem. The probability of error for a well design soldering task performed by a highly motivated technician might be in the region of 10^{-4}. This would be regarded as a very high level of human task reliability by human factors specialists. If statistical independence between each solder task is assumed, the probability of an error for 100 joining tasks would be in the region of 10^{-2} (100×10^{-4}). If, however, the technician is inexperienced the probability of a single error could increase significantly. If the probability increased to say 10^{-3}, the probability of a single error in 100 soldered joints would then increases to 0.1. While these numerical values may be discounted as little more than guesswork they do at least serve to illustrate the important point that in manufacturing, where the tasks are dependent on the skill of the operator the possibility of a fault arising from human error can escalate especially where there are large numbers of tasks to be performed. A high level of quality control by well trained and motivated staff is essential in manufacture and assembly of the vehicle.

These manufacturing quality issues were well appreciated by the AUV developers. Hence the decision to mostly use contractors to assemble in-house designed PCBs, the use of crimp terminals rather than soldered terminals in wiring looms, and the use of Quality Control procedures as described in 6.1 (Hardware Quality Control).

Integration of Science Packages: While, in principle, science packages should be designed such that they do not affect the control and operation of the delivery vehicle, in practice their performance can have an effect. For example, package failure may create additional current demand causing more rapid battery depletion. The science package integration task is understood to be a problem for the design team in that "unfunded" effort (sometimes the level of effort is significant) is expended trying to resolve snags and problems associated with the science package. This can divert the team's effort away from vehicle design and manufacturing tasks and from reliability achievement.

Field Operation: Once the system is operational, the system is exposed to the effects of the environment. At this stage vehicle reliability is primarily influenced by operator actions, operator errors e.g. in programming the mission details and in the environment encountered. The reliability of the operator's actions can be addressed but the environment is largely unknown and outside the control of either the designer or the operator.

Maintenance: A number of routine and in some instances non routine maintenance tasks may be needed to keep the AUV operational. For example, some of the connectors need to be tightened between missions. This is a human task and as a result is subject to human error, compounded in some instances, by access difficulties and lack of tightening tools. This is an obvious source of errors, faults and defects. The probability of human error in a maintenance task performed at sea on the mother ship will be much greater than a similar maintenance task in the comfort of the laboratory back on land.

System Upgrades: The AUV Systems are from time to time upgraded to make performance and reliability improvements and in some cases to accommodate science package changes. Such changes often involve a degree of design effort and system reconfiguration both at software and hardware level. Any changes made are a potential source of uncertainty, loss of reliability and hence risk. However, it should be understood that the need to improve

system reliability may also require design or manufacturing changes. The risks and benefits of such changes must be managed carefully to meet the overall project goals.

The AUV teams are well aware of these issues, and think long and hard to assess the risk versus benefits of any changes, especially in field operations situations where the opportunity for extensive field testing could be limited.

7 Organisational and Risk Management Issues

Although the root cause analysis above provided insights into the technical root cause of the failure, it has not been possible to come up with a strong candidate for the actual cause of failure, only possible causes. This is disappointing but expected and unavoidable because of the limited amount of information available on the state of the system during the mission particularly at the time of failure. However, whilst, it is important to understand the technical causes of the AUV failure as part of the lessons learnt, it is arguably more important to address how the risk of any failures causing loss of the vehicle can be minimised in the future. This has far more to do with risk and reliability management of future AUV development programmes and is addressed in this section of the report.

The "under ice" AUV project is one of the most challenging from a risk and reliability point of view. Because the AUV is a key element in delivering the NERC marine environmental research programme the technologies involved tend to be relatively novel and cutting edge and the environments in which the technology is deployed, especially those under ice, are demanding. The risks are significant. The probability of a system failure causing immobility of the AUV, although undefined at this stage, is believed to be high and may well be greater than acceptable to NERC and the AUV user community.

This latter statement of course begs the question of what is an acceptable risk of loss of the AUV and to a large extent this question depends on the consequences. While the AUV is operating under ice the consequences of a failure are significant because, unlike open water, it cannot be raised to the surface to retrieve it. Essentially the AUV is lost if the system fails. This has an immediate financial impact in the range of millions of pounds, important data is lost and although there will be other opportunities to gather data it will be at additional cost and delays which may be of the order of months to years. The losses will be felt by all the research students and scientists whose research is dependent on the successful acquisition and return of data from the AUV. There is also the intangible, but no less important, consequence of reputation loss which will be felt by the NOC and NERC.

7.1 Good Risk and Reliability Management Practice

In this section we review a number of risk management issues pertinent to the AUV development programme and which will serve to guide recommendations to NERC on the management of risk in future projects. Figure 6 shows a slide with key activities in risk management.

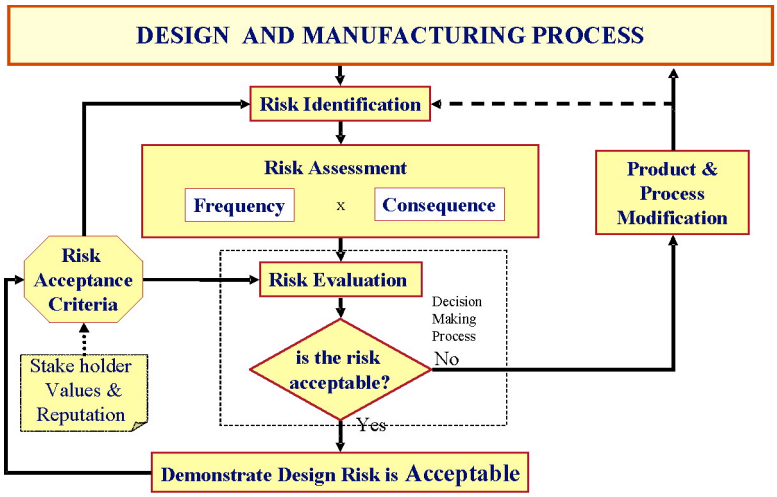


Figure 6: Schematic Risk Management Process

An important starting point for this process is to understand what we mean by risk and then to define appropriate risk acceptance criteria for the project or the system.

Definition of risk: For the purposes of this report we define risk as the product of probability and consequence of a defined event. In the context of the AUV project, an important event to consider is the loss of the AUV under the ice shelf. The consequence of this event includes the loss of the vehicle and data. Some of this loss can be quantified in financial terms but the wider implications of the loss are difficult to quantify, for example, the impact on student theses and researchers reports which may be dependent on delivery of data from the AUV and the loss of the data on environmental decision making in the short term.

Risk acceptance criteria and reliability requirements: It is good practice to define risk acceptance criteria. This is a key input to decision making. For if numerical risk acceptance criteria are set, this can be converted to a system reliability requirement which would drive the AUV team assess the system risk and reliability and, in turn, take appropriate design and manufacturing actions aimed at meeting the systems reliability requirements, as far as it would be practical to do so.

Risk identification: The first step in creating a reliable system is the process of risk identification which involves the identification and understanding of the numerous failure modes and mechanisms by which failure can occur. It is a vitally important first step, since a risk not identified is a risk not assessed or managed. Risk identification (failure modes and consequence criticality) is the first step towards reliability improvement. Standard tools such as design FMECA and process FMECA are available to support this. A good understanding the root cause mechanism of the failure mode is an *essential* requirement for reliability improvement and risk reduction.

Risk and reliability assessment: The assessment of risk and system reliability of AUV systems is an important input into judging the acceptability of a given design configuration. However numerical system reliability analysis is often contentious with designers due to lack of good data, consumption of additional engineering time and lack of reliability expertise being cited as problematic. This leads design teams to resist requirements to perform numerical reliability modelling. However, many of these problems can be overcome with time and directed effort to collect and analyse data. Numerical systems reliability assessments provide valuable insights into potential system reliability performance and how this is related to design configuration and component reliability. It is important to develop the capability of designers to quantify risk and reliability.

It is worth noting that even if fully quantitative approaches are rejected as not practicable, semi-quantitative risk assessment can be useful. For example a failure modes and effects criticality analysis (FMECA) can be performed with limited data, using primarily the knowledge and expertise of the designers to make judgements on the level of risk. Identification of system cut sets and qualitative importance analyses can also hep focus design and manufacturing attention to where reliability improvements can be implemented and add value.

Reliability improvement and risk reduction: Reliability is achieved by eliminating failure modes, or by reducing their probability of occurrence. This can *only* be achieved by a high level of understanding of the causes of each failure mode. The consequence dimension of risk is important in judging the acceptability of the probability of a failure mode. For instance a failure mode which results in the complete loss of the AUV logically should have a much lower probability of occurrence than a failure mode which only causes loss of data. In developing risk reduction measures, it is also important that the design team addresses not only the probability of failure mode occurrence, which requires a deep knowledge of the failure mechanism, but also the consequences of failure. For example a number of faults were designed to trigger system Abort after 20 seconds hold off time, a simple configuration change to a longer time could reduce the fault consequences. For under ice activities the design team should investigate more robust design features to enable the AUV to return to the Mother ship as a simple surface and retrieve strategy is not viable. Risk assessment and the imposition of risk acceptance criteria are important in driving the designer's attention to consider and develop alternative retrieval options.

NOCS AUV team Use of Reliability Management Methods: Throughout this review the Board has recognised the competence and commitment of the NOC AUV team; they have a high level of understanding of the importance of reliability and have employed sound reliability principles to influence their design decisions. However, they have not employed any formal systems reliability analysis methods. The Board believe this to be a major shortfall. There are a number of key processes that are important in reliability management. These provide the basis for good risk management practices that should be implemented by the AUV developers and which have implications for the NERC.

7.2 Key Risk and Reliability Processes

The risk and reliability strategy described below is based on that which is currently being developed by the subsea oil and gas sector and is considered a useful model on which to base the discussion on how NERC might manage risk in future AUV related projects.

The reliability strategy is based on developing key processes, comprising four core reliability processes and ten reliability implementation and longer term reliability management processes.

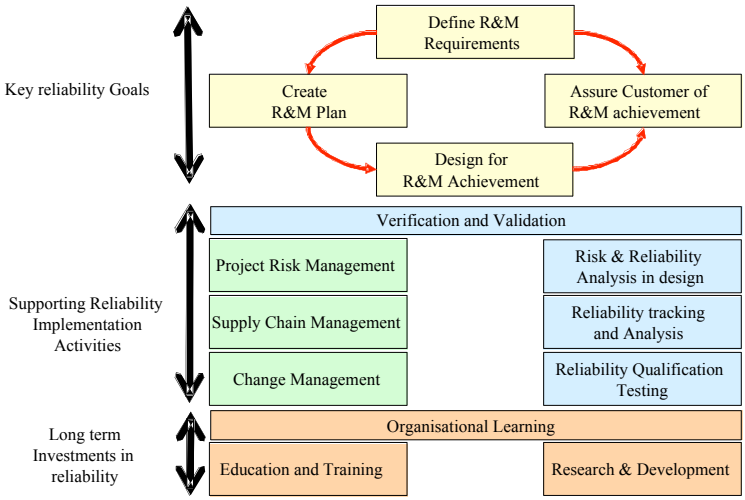


Figure 7: Key Risk Reliability practices

The key goals of the reliability strategy are:

1 Define R&M[§] requirements and risk acceptance criteria
2 Create R&M plans (addresses R&M tasks, design tasks, timings and teams)
3 Design a system which delivers the R&M requirements (*Design for R&M*)
4 Provide evidence of R&M achievements (*R&M Case*)

Define R&M Requirements: Risk acceptance criteria are in effect an input to reliability requirements. Mathematically this can be estimated as: P* = Risk* / Consequence, where P* is the required probability of occurrence of a defined event (such as loss of vehicle), Risk* is the level of risk that can be accepted or tolerated by the stake holders. The latter may be linked to an insurance premium, but in practice is more likely to be a group decision based on a variety of factors. The lower the level of risk that can be tolerated and the larger the consequence of the failure, the lower is the target probability of failure (higher reliability requirement).

R&M planning: R&M planning is an important first step in implementing a reliability strategy. Planning should identify the R&M tasks to be performed as well as the engineering actions necessary to achieve reliability. It should identify when tasks are to be implemented and the resources necessary to perform the tasks.

Design for R&M: It is important to point out that reliability should be mainly concerned with engineering. Analysis helps engineers to "identify the failure modes" and to "measure" the level of reliability achieved, it is engineering that actually delivers reliability. To this extent the analysis is used to support engineering decision making. Design for reliability is the process of implementing design actions which bring about the reliable system.

[§] R&M is the acronym for reliability and maintainability. It includes availability and logistics issues

Evidence of Reliability Achievement: A number of organisations are now asking for documentation with information supporting the reliability claims of a supplier. This is increasingly used as a contracting tool between a customer and a supplier. The Ministry of Defence have adopted this approach for certain high risk military development contracts. The output is a document called an R&M Case. In the subsea industry a similar approach is being used. In this sector the document is called a Reliability Demonstration Document.

Risk and Reliability Implementation and Reliability Investment practices:

In addition to the above, there are seven supporting risk/reliability management activities that are important in the implementation of reliability in development projects and three longer term processes which can be considered long term investments in reliability. It is inappropriate to describe these processes here. However, they are listed as examples as good organisational practices in implementing reliability and risk management.

1 Verification and validation (of R&M tasks,, models and data)
2 Reliability planning and project risk management
3 Supply chain management of reliability
4 Management of Change and life cycle transitions
5 Application of Risk and Reliability modelling/analysis in design
6 Reliability performance tracking and data analysis
7 Reliability and qualification testing

Long term investments in reliability:

8 Organisational Learning from feedback and analysis of lessons learnt from failure
9 Education and Training in risk and reliability analysis and management
10 Research and Development of reliability assessment and improvement methods

These key activities should be seen as an integrated whole. There are however different emphases at different times throughout the life cycle. One of the reasons for developing plans is to ensure that reliability activities focus on the relevant issues at the different stages of the development process. For example during conceptual design phases there is more emphasis on systems reliability assessment. In detail design phase there is more attention to the reliability of components, especially failure critical components such as seals. FMECA might at this stage focus on both the product (design FMECA) and the manufacturing process (Process FMECA). In the case of the latter, the analyst identifies failures in the manufacturing or assembly process which could result in a defect or a failure in the system. For manual assembly operations the latter may well involve consideration of human reliability and task competence.

7.3 Implications for the NERC

The purpose of the Natural Environment Research Council is to deliver independent research, survey, training and knowledge transfer in the environmental sciences, to advance knowledge of planet Earth as a complex, interacting system. Its work covers the full range of atmospheric, earth, biological, terrestrial and aquatic sciences, from the deep oceans to the upper atmosphere, and from the poles to the equator. Its mission is to gather and apply knowledge, create understanding and predict the behaviour of the natural environment and its resources, and communicate all aspects of our work. It is a non-departmental public body, funded by government via the Office of Science and Technology and is accountable to the public for the work that it does and the way that it is implemented.

Risk Management is central to NERC's approach to managing research projects. However, there are a range of responsibilities and approaches that may be adopted, depending on the scale of the risk. The first point to note in the context of the *Autosub under ice programme* is that this is *a high risk project* in which it is clearly possible for the vehicle to be lost and irretrievable. There is little documented information on any prior risk assessment made, although there must have been consideration given to this at some stage as the vehicle was covered by insurance. There are two areas that NERC might address:

- The setting of risk acceptance criteria on high risk projects
- Its approach to the management of risk in projects

In general terms, NERC may consider or adopt one or more of the following generic risk management approaches in its science projects:

- Avoid the risk entirely (e.g. by NERC not funding such high risk projects)
- Reduce risk by reducing the probability of events that cause losses (imposed on the project team)
- Reduce risk by reducing the consequences of failure events (imposed on the project team)
- Transfer the risk, e.g. by purchase of insurance
- Accept the risk

As discussed in section 7.2 above, the setting of risk acceptance criteria initiates activities to manage risk and it is recommended that NERC investigate procedures for this where the projects are high risk. The form of the acceptance criteria will vary from project to project and is difficult to define in advance. However, there are three general approaches that can be adopted, namely for NERC to require:

- **Risk Assessment and Management Capability**: Proposals should demonstrate that the research team has effective risk assessment and risk management capability. In the case of the AUV project, where the risk of loss is closely linked to the reliability of the vehicle, proposals should demonstrate that the research team have good reliability assessment and reliability management capability.
- **Technical Risk acceptance criteria**: In the case of the AUV it is considered appropriate for NERC to consider setting a numerical level of risk that is acceptable. For example; it may desirable to limit the probability of loss of the AUV to less than 0.1 over the project life time. This criterion can then be translated into a minimum system reliability requirement, given knowledge of the number of missions to be run in a research programme. For 10 missions, this could be translated into a minimum system reliability of say 0.99. It would then be up to the design team to demonstrate that this reliability can be met for the programme. There may be a need for some negotiation between NERC and the project team to reach an acceptable division of responsibility.

  Note: The probability may be linked to an insurance premium. For example, if the insurance cover for the loss of the vehicle costs NERC £X and the financial loss to NERC if the event occurs is £Y, then the probability of the event P* should be less than X/Y. If NERC is to cover the loss then X is the amount of loss that NERC would be willing to sustain.
- **Risk or Reliability Assurance**: Prior to deployment of the vehicle, NERC should consider imposing a requirement on the design team to provide evidence that the AUV has an acceptable reliability. In order to implement this requirement in a project, the project would have to proceed through at least one decision gate say at the end of design but prior to manufacture and possibly a second gate immediately following manufacture and prior to operation. NERC would then have the final decision to go ahead with the missions or to require changes.

8 Conclusions

The following conclusions can be drawn from this investigation:

1 **In consideration of Circumstances surrounding the loss of Autosub2**

1.1 The inquiry board has reviewed, in detail, the available information and documents concerning the circumstances surrounding the loss of Autosub 2 under the Fimbulisen in February 2005. The loss occurred during mission 383 which followed the well established operational procedures used successfully on numerous open water missions and in the previous under ice mission. The Board accepted that the loss was caused by a technical system failure.

2 **In consideration of Possible Technical Causes of Failure**:

2.1 A comprehensive analysis has been made of the technical reasons for the loss of the AUV. However, because it has not been possible to recover the AUV from under the ice shelf for direct examination of failure, it has not been possible to identify the actual technical root cause of its loss. Consequently an assessment has been made of the likelihood of different failure modes causing the loss. The output from this activity is summarised below

2.2 The review team felt that the loss was equally likely to have come about from an *Abort Command* (AC) as a *Loss of Power* (LP). The most important failure modes causing these events and their likelihoods being:

Cat	N	Failure Mode	Likelihood
LP	1	Open circuit h/w failures	28.5%
AC	2	Network fails for t>20s	23.8%
AC	3	leak sensed for t>20s	20.4%
LP	4	Short circuit h/w failures	9.5%
LP	5	loss of connectivity	7.1%

There is 89% likelihood that the true cause of failure falls within one of these five categories. There is 73% likelihood that the cause was one of the three failure modes; open circuit failure, network failure or leakage failure. The possibility of a joint event causing loss of the AUV was considered possible but unlikely (5%). Loss of power by open circuit network failure was considered the most likely cause of failure at 29%, followed by an Abort commanded from a network failure at 24%. Network failures, in both the dry and wet domains were the most likely sources of loss of power followed by connector, joint and seal failures. The most likely causes of an abort command were considered to be failures of; wiring on the printed circuit board, current sensing resistor, in-rush current protector, dc-dc current converter, magnetic switch and main power switch. Table 5 in the main report summarises all the possible failure modes and their likelihoods.

2.3 One member of the board, Dr Albert J Williams 3rd, took the view that the most likely cause of failure in his experience was the water ingress into one or more of the Burton 4 pin Connectors causing an Abort Command. The justification of this conclusion is outlined in annex 4, which is a letter communicated to the Board members following the submission of the first draft of the report. As an acknowledged domain expert, these views must be greatly respected. However, although the Board agreed that sea water ingress was a very strong candidate for the actual cause of loss, there was no direct evidence that this was in fact the cause. As can be seen from the table in conclusion 2.2, when all the views of the Board were combined in the failure analysis, although there was not a large difference in the likelihood among the top 3 causes of

failure, leakage failure was 3rd largest. The AUV team have recently carried out extensive pressure cycle testing of these types of connectors. These tests have revealed no problems due to water ingress.

2.4 An assessment was made of the source of the failure. The approach taken was to assess the likelihood that a failure mode originates during a particular life cycle phase. The analysis indicates that the source of the failure was most likely to have been a fault introduced during the manufacturing/assembly phase (52%), followed by Maintenance (25%). Design error was considered less likely (14%) while Operations (7%) and External factors (1%) were considered least likely. This indicates that the greatest benefits to reliability improvements are most likely to come from attention to faults originating in the manufacturing and assembly stage, followed by attention to faults arising from maintenance activities.

3 In consideration of AUV loss risk mitigation

3.1 Although the probability of an AUV fault causing a system abort or loss of power has not been estimated in this review, it is believed to be significant. It is recommended that in future AUV developers perform quantitative systems reliability assessments routinely during design and development to support design and manufacturing decision making.

3.2 Because it is virtually impossible to retrieve the AUV if a system fault or failure causes immobilisation. The risk of AUV loss is much higher when deployed under the ice than when deployed in open water.

3.3 It is highly desirable that the designers reduce the risk of under ice missions by taking appropriate measures to:

- **Reduce probability of failure:** risk can be reduced by making any event that might cause a loss of power or trigger an Abort less probable. This goal will demand greater emphasis on designing for robustness and reliability and on developing screening tests to reveal faults before the start of a mission.
- **Assess mission risk and AUV system reliability:** In future studies it is suggested that numerical estimates be made of system reliability to focus design attention on the need to reduce risk to an acceptable level and to support design and mission operation decisions.
- **Reduce the consequences:** It is necessary to investigate the options for developing improved measures to enable the AUV to be retrieved or to "limp" home in the event of a failure under ice.
- **Retrieve fault condition data:** Information on the fault states of the system and the timing of failure events during a mission is important if the system developers are to learn from failure and develop corrective actions. The means of transmitting this information from a stranded AUV to the mother ship should be developed.

4 In consideration of Short comings in AUV design Management

4.1 It is clear that the development team at NOC have a high level of design skill and have adopted a sound and structured engineering approach to the development of the AUV. Reliability considerations have also informed design decisions through good systems engineering practices, but the team have no formal reliability or technical risk assessment procedures implemented to support design decision making. This is considered to be a major management weakness.

4.2 Reliability analysis should be implemented wherever this can aid engineering decision making. The following is considered the minimum for this type of project

- Implement technique for the identification and assessment of system technical risk. Typical good practice is to perform "design FMECA" and "process FMECA"

- Implement techniques to understand the level of system reliability achieved. Appropriate systems reliability tools include; reliability block diagrams/network analysis, Fault tree analysis and event tree analysis.

4.3 Although the AUV development team are not responsible for and have no control over the design of science packages, they are responsible for integrating the science packages into the AUV. Interfacing and incompatibility problems are frequently encountered. The resolution of these problems, many of which are outside the direct control of the AUV team, has considerable impact on staff resources and the diversion of team effort.

4.4 Due the large numbers of connections and leakage paths, it is necessary to pay particular attention to the reliability of electrical connectors and harnesses. A high level of quality assurance in manufacture and assembly is required.

5 In consideration of Improvements to Autosub Risk management procedures

5.1 The *Autosub under Ice Programme* is a high risk project. In the event of a failure causing the vehicle to become immobilised it would be difficult if not impossible, to recover. It is recommended that NERC should require design teams to implement good risk management practices aimed at preventing a future AUV loss or reducing the risk of loss to a level acceptable to NERC. Good risk and reliability management practices should address the following key objectives; (i) definition of risk acceptance criteria and R&M requirements, (ii) Creation of plans for the assessment and achievement of reliability (iii) Implementation of design, manufacture and assembly activities, to achieve risk and reliability targets, (iv) implementation of risk and reliability activities to support design decision making and (v) provision of evidence of reliability achievement. Other supporting reliability implementation processes listed in section 8.2 are considered useful and are recommended as good practice.

5.2 The ability to identify AUV system failure modes and to forecast the system reliability is an important capability in *design for reliability*. Standard, well proven methods are commercially available to support this type of work. Two approaches are commonly used in industry; Failure Modes and Effects Criticality Analysis (FMECA) which can be used to identify component failure modes and systems reliability analysis employing Reliability Block Diagrams or Fault Tree Analysis. Both of the latter techniques can be used to model and assess a system to identify cut sets and quantify cut set probability.

5.3 The achievement of a high level of system reliability for the AUV is a significant task requiring considerable attention to the practical issues of joint, connector and seal reliability. There are large numbers of connections and seal paths and the failure of anyone can trigger a system fault and a failure event. While reliability improvements can be made by building in redundancy, the opportunity for this may be restricted by space and design limitations and where it can be implemented reliability may be compromised by the additional complexity that redundancy introduces. The design team are also constrained by some of the bought-in items, the reliability of which is outside their direct control. It may be difficult, therefore, to achieve a high level of reliability and that NERC may therefore have to accept a significant risk of a future AUV loss. The procedures suggested in 5.1 and 5.2 however, will mean that the level of reliability achieved will be better known and understood and this will enable better insurance arrangements to be made.

6 Options for NERC Risk Management

6.1 NERC should consider implementing a rigorous technical risk management regime on high risk AUV projects. In particular, NERC should

- Develop appropriate methods for defining project risk acceptance criteria which can be translated into AUV system reliability requirements.
- Require the AUV development team to develop and implement good risk and reliability assessment and management practices.
- Require projects to provide assurances to NERC that reliability requirements can be met in advance of operation

9 Recommendations

The key recommendations from this AUV loss review Board relate to the need for implementation of stricter risk and reliability management practices in high risk AUV projects. These management recommendations are outlined below in 9.1. A number of technical design recommendations which will impact on AUV system reliability are outlined in 9.2 below.

9.1 Risk Management Recommendations

1 NERC, or their authorised representatives, should define risk acceptance criteria for future high risk AUV projects. These criteria should be capable of being translated into reliability requirements for the AUV development team to meet.

2 The AUV development team should be required, as a condition of contract, to develop capabilities in risk and reliability assessment and management and implement these formally during the development of the AUV and its subsequent operation.

3 The AUV development team should provide evidence of reliability achievement in advance of operation

9.2 Technical Design change Recommendations

There are a number of technical design changes, leading to improvements in system reliability, recommended by the design team shortly after the loss event. These are listed below. Many of these have already been implemented[4].

1 The battery system is vulnerable to a single harness short circuit or short circuit in a single battery tube. This could cause total power failure. Diodes should be wired in series with each of the four battery power inputs within the management pod.

2 There are many systems vulnerable to interruption or failure of the 48 volt power bus. It is recommended therefore:

a) To change of power supply architecture to use 4 wires, thereby providing dual redundancy of power supply for critical systems. Non critical systems cannot short circuit both supplies.

b) To group critical systems close together on the network and have local capacitive energy storage on 48 volt supply to critical systems. 2000 micro Farads would be adequate for 0.5 second power hold up.

3 The network is vulnerable to an Abort failure because the abort timeout was set very short. It is recommended therefore to change "abort hold off" time from 20 seconds to 10 minutes default.

4 Critical systems and abort system are vulnerable to interruption of the network. It is recommended that critical systems are grouped close together on the network.

5 It is recommended that if technically feasible, dual redundant wiring should be used by for the network to increase system reliability.

6 Wiring and connectors are vulnerable to mechanical damage during assembly. This issue should be addressed in future Autosub designs with particular attention being paid to wiring protection and strain relief. Wires should be routed to avoid snagging.

7 A subset of the bulkhead connectors on the vehicle are difficult to tighten. It is recommended that

a) Special tools be developed for tightening connectors to meet a specified torque requirement in difficult to reach areas.

b) Designers should investigate the possibility of a design modification to the bulk head connectors to enable mechanical pressure to be applied when the hydrostatic pressure is low

8 There are some uncertainties about battery discharge curves and the effect of variable discharge rates of battery pods.

a) Test procedures should be developed to reduce these uncertainties.

b) AUV design should take account uneven battery discharge rates, or develop technical solutions which ensure better current sharing.

9 Technical information on failures occurring in service is limited because record keeping of the fault log on the Autosub is intermittent. The AUV operation team should implement improve recording procedures.

10 All the configuration variables for Autosub system are not automatically recorded. There is a need therefore for a tool which records the whole system configuration for the vehicle before mission start.

11 Although it is possible to infer vehicle position from the emergency beacon, it is not currently possible to transmit information on the cause of the failure because the Information Emergency Beacon data mode is not used in an emergency. This data mode was not used because tests on previous missions had showed that the ranging information could be corrupted by the data transmission and so the software for decoding the message was never developed. It is recommended that this issue be revisited.

12 The Mission control exception event and event set up is confusing and error prone. The problem is compounded by the need to manually enter settings for each power up. It is recommended that the "mission configuration" incorporated into the mission scrip itself.

13 Wrong configuration settings could have as serious consequences as wrong mission script. It is recommended that a double check of the configuration is placed on the checklist as is the case for mission script.

14 The mission control node duplicates the mission timeout, and the maximum depth abort settings, which are already covered in the release nodes. This duplication adds additional complexity and hence an unnecessary vulnerability. It is recommended that these settings are disabled.

15 It is recommended that the design team investigates options for developing a "limp home" capability to enable the AUV to be retrieved in the event of a critical systems failure under ice.

10 References

1. NERC Thematic programme Proposal, *Processes beneath the Ice shelves: Autosub investigation and implications for the linked ocean-ice climate system,* (grant ref number)

2. G Griffiths, N W Millard, S D McPhail and J Riggs: *Effect of Upgrades on the reliability of the Autosub AUV;* Proceedings of Unmanned, Untethered systems Technology Conference, New Hampshire, August 2003

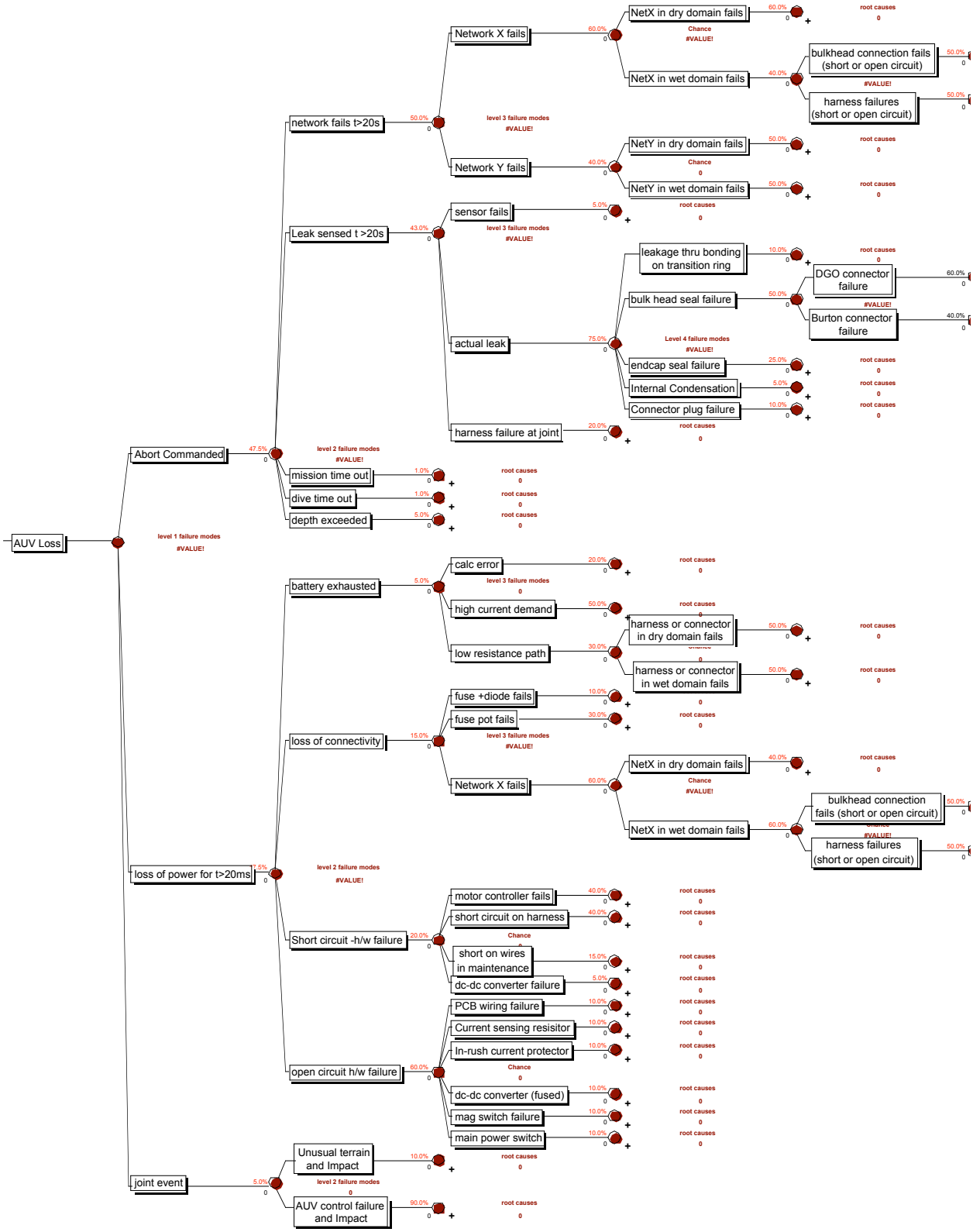
3. G Griffiths, N W Millard, S D McPhail, P Stevenson and P G Challenor: *On the reliability of the Autosub Autonomous Underwater vehicle;* Journal of the Society of Underwater Technology **25**(4), 175, 2003

4. S D McPhail: *Analysis of the Loss of the Autosub mission 838 on 16th February 2005 beneath the Fimbulisen;* Report created on 31st March 2005.

5. J Copley; *Autosub Under Ice Risk Register* ; Original Report created 11-02-2004 {updated by Ken Collins 20-7-04}

Annex 1 Root Cause Tree

This tree has been produced with the Technical Root cause branches at the ends of the trees collapsed (+) to enable the text on the main braches to be visible.



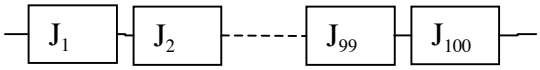
Annex 2 AUV Systems Reliability Issues

While this review has attempted to identify potential causes of failure which would result in the loss of the vehicle, it has not attempted to make a formal assessment of the probability of failure. However, it is pertinent to address the question of the potential probability of AUV loss during a given campaign. The following paragraphs are a discussion of reliability issues.

In any assessment of system reliability, the failure logic of the system is critically important. In the AUV control system there are a large number of joints and connectors and these are fundamental to the design philosophy. It is understood that the failure of any one of these joints or connectors would cause a system fault or would cause a loss system redundancy (in the case of a redundant system). As discussed under the failure analysis section, a leaking wet connector could cause failure as could a dry joint or a short circuit. Although there is redundancy designed into the system, the AUV system has long chains of connected components and nodes in series. The system is therefore vulnerable to such failures especially those introduced during assembly and maintenance.

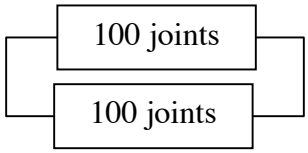
As implied by the failure analysis, there are 3 high level system failure modes which could lead to immobilization of the vehicle, these are; System Abort, Loss of Power and Joint event trapped AUV. Each has a probability of occurrence and the overall probability of failure of the system is, to a good approximation, the sum of the probability of these failure modes. (It is exactly equal where the 3 failure modes are mutually exclusive and independent).

In practice the probability of failure will be dominated by the two "control" related modes, i.e. Loss of power and System Abort, which involve large numbers of components. The following simple calculation is used here to illustrate the impact of joint numbers on system reliability. This estimate assumes that the failures occur at random.



Suppose the number of joints in series is 100 and suppose the each joint has a failure rate of 100 failures per million hours. This would provide each joint with a 10 hr mission reliability of 0.999. This figure seems reasonable until the system reliability is calculated. If any of the 100 joints could cause system failure then the system probability of failure on a single 10 hour mission is approximately 0.1. If 10 missions are to be run as part of a campaign, the probability of a failure during the 10 mission campaign would be 0.63.

The reliability of any system can be increased by introducing redundancy in the system. The impact of this can be significant. For example in the example above, if the 100 joints were duplicated so that the system was that shown in the diagram below described below, the probability of system failure during a 10 mission campaign would decrease to 9%. This is still a high probability of system failure and could be greatly increased (up to that of a non redundant system) if there were common-cause failure mechanisms present defeating the designers intent. One might, therefore reasonably question whether this is an acceptable probability for under ice AUV campaigns.



Annex 3 Description of Lon works and CSMA

Lonworks is a protocol developed by Echelon Corporation for manufacturers who wish to use an open protocol with off-the-shelf chips, operating systems, and parts to build products that feature improved reliability, flexibility, system cost, and performance. LonWorks technology is accelerating the trend away from proprietary control schemes and centralized systems by providing interoperability, robust technology, faster development, and scale economies.

A major goal of LonWorks is to give developers, from the same or different companies, the ability to design products that will be able to interact with one another. The LonWorks protocol provides a common applications framework that ensures interoperability using powerful concepts called network variables and Standard Network Variable Types (SNVTs).

Communication between nodes on a network takes place using the network variables that are defined in each node. The product developer defines the network variables when the application program is created as part of the Application layer of the protocol. Network variables are shared by multiple nodes.

The use of Standard Network Variable Types (SNVTs) contributes to the interoperability of LONWORKS products from different manufacturers. If all manufacturers use this variable type in their application when a network variable for continuous level is defined, any device reading a continuous level can communicate with other devices on the network that may be using the variable as a sensor output to initiate an actuator.

CSMA is short for Carrier Sense Multiple Access / Collision Detection. CSMA is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). Standard Ethernet networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval the stations that collided will attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

CSMA/CD is a type of contention protocol. Networks using the CSMA/CD procedure are simple to implement but do not have deterministic transmission characteristics. The CSMA/CD method is internationally standardized in IEEE 802.3 and ISO 8802.3.

Annex 4 Preliminary Conclusions from Albert J Williams

Dear Professor Strutt, members of the Autosub Loss Review Board, Dr. Beadman, and Autosub Team

The draft Autosub Loss Review Report is an excellent and comprehensive document. It examines in a comprehensive way the risks in the Autosub Under Ice program and serves as a valuable guide to design, manufactured part assurance, assembly, maintenance, repair and replacement procedures, operation, and, in general, the accounting for and planning for reliability. I have learned a great deal from this analysis in my own work. I applaud the comprehensive treatment of all or most of the systems of Autosub (and the environment) in the context of the failure resulting in its loss.

The specific and immediate cause of the loss on mission 383 in my opinion is water ingress into one or more of the 68 Burton 4-pin connectors caused by pressure cycling between 250 meters and as much as 700 meters without connector locking ring tightening between cycles. While this is only an opinion of an old hand at underwater instrumentation, it would be a waste of effort if this did not get included in some way in the overall record of the Autosub Loss Review. I would be satisfied if this e-mail attachment were simply distributed with the report or included as an Appendix. My reason for wanting this inclusion is that it leads to a suite of tests and possible corrective actions that are not obvious in the draft report.

To justify my conclusion that water ingress into one or more Burton connectors may have occurred on mission 383, I start with the observation of the design of the connector. It has no O-rings excluding water from the pins, relying instead on axial compression of a rubber moulded shape against a metal rim. The initial means of compression is a locking ring while at depth, hydrostatic pressure maintains this seal. The area of the sealed cavity against which pressure works is about 2 square inches and at 250 meters depth the pressure is 25 bars or 367 lbs/sq. in. Thus, the force keeping the connector closed is at least 700 lbs. But the pressure cycling is more than that and the report by the operators is that after each deep mission of Autosub, each locking ring could be tightened and was routinely re-tightened before the next mission. This is an indication of deformation of the rubber part (expected) and possibly of cold flow (unexpected) that is progressive. I am therefore concerned that repeated cycling without re-tightening of the locking ring may lead to deformation of the connector to the point that water may enter. The major difference between mission 382, successful, and mission 383, failure, was this pressure cycling from the yo-yo dive profile. So we have here a mechanism and a cause for connector deformation and possible failure.

The consequences of water ingress into any connector are covered in the draft report. Loss of network or loss of power is the expected result of water in a connector and either of these losses will trigger an abort condition. The abort is safe and the most desired response in open water but fatal under ice.

I recommend that exhaustive tests on the Burton connector, or another connector that might be used to replace it in future designs be performed. Such tests should be run with bends in the cable near the connector that are characteristic in cable connections and that may exist in Autosub. Pressure tests should cycle the connector in seawater from, for example, 10 bars to 100 bars, 100 times, and include checks for electrical leakage between pins. As explained in the draft report, individual component reliability must be extraordinarily high to achieve even moderate reliability when components are in series and failure of only one component may imperil the system. I would suggest that the actual set of connectors to be used be wired in series and so tested to gain confidence in the design and safety in the application and to test each individual connector for defects in manufacture. This quality assurance is most important before an Autosub under ice mission where the abort procedure may be fatal.

While this concludes my analysis and recommendation, I would like to share a career's worth of underwater connector experiences of the worst kind to illustrate why these components are almost always the weak link in an underwater instrument. And, I might point out, that in manned submersibles and some ROVs, connectors are replaced by soldered wiring in pressure exposed oil-filled tubes. As Professor Nam Suh of MIT explained in his theory of orthogonal design, it is best to have as many features in a design as requirements, so that each can be optimized without impacting the others. An underwater connector is an extreme violation of this principle since pressure resistance, water exclusion, electrical conductivity, and electrical isolation are accomplished with only one

or two features rather than four. The Burton connector is probably fail-safe in the sense that it can resist pressure even when the seal fails but suffers from combining water exclusion with electrical isolation.

Electro Oceanic underwater pluggable connectors, popular in 1970, and available today as IE connectors from Impulse, suffered from intermittent electrical contact due to two causes: stretching of the brass or stainless rings of the socket and breaks or crimp failure in the wire to connector mold. The failures were exhibited as high resistance through the circuit and/or a pressure-related opening of the circuit. In some cases, those with a magnetic reed switch molded into a cable termination, pressure caused an apparent switch closure due to a void in the molding between wires. Pressure collapsed the void, shorting the wires.

The wet-mateable IL/BH connector from Impulse and Sea Con is a descendant of the Electro Oceanic connector, originally developed by a former employee to get around the EO patent. It suffers as we both know from becoming open circuit sometimes under pressure, possibly from grease being hydraulically pumped into the contact area and expanding the socket.

The O-ring sealed glass reinforced epoxy series XSJ, XSE, and XSJ type connector depend on two O-rings and a locking sleeve to engage the first O-ring. After that, the face O-ring seals the electrical cavity. But manufacturing changes in one experience I had caused the second O-ring to not seal. Numbers were stamped into the mold where the O-ring seat was located but worse yet, the length had been shortened, so that the connector bottomed out before the O-ring reached its seal. While reliable in general, this connector is vulnerable to as little as one drop of sea water in the electrical cavity causing a shorting of the pins. The pins are not individually isolated, just as in the Burton design.

The XSG and LSG-type underwater connectors have a rubber sealing shell over exposed pins extending from a hard plastic bulkhead connector. The rubber shell seals against water ingress but, in addition, each pin is separately sealed from the others, by a contact line at the base of the pin where the rubber is hydrostatically pressed against a ridge at the pin base. These connectors, although vulnerable to having the pins bent during maintenance, have given me the least difficulty underwater. By contrast, an inverted version of this connector with sockets in the hard plastic bulkhead connector, VSG type, fail almost 100% in several years of service through stretching of the sockets.

I have begun using a rubber plug in metal socket connector of the IE55 type without O-ring, not from belief in its superiority but to benefit from its small size. Ostensibly, the rubber is forced into the cavity by a locking ring, as in the case of the Burton connector, but the rubber in these connectors appears intended to fill the volume. I don't know if these connectors are reliable yet, having experience with only 20 instruments deployed for a year at a single depth of 2300 meters, one connector each, and a single deployment plus three test pressure cycles before deployment. Although they did not leak, the range of exposure is too limited to recommend them. Nor is the pin size sufficient for Autosub current capacity.

Submitted by Albert J. Williams 3rd
Autosub Loss Review Board