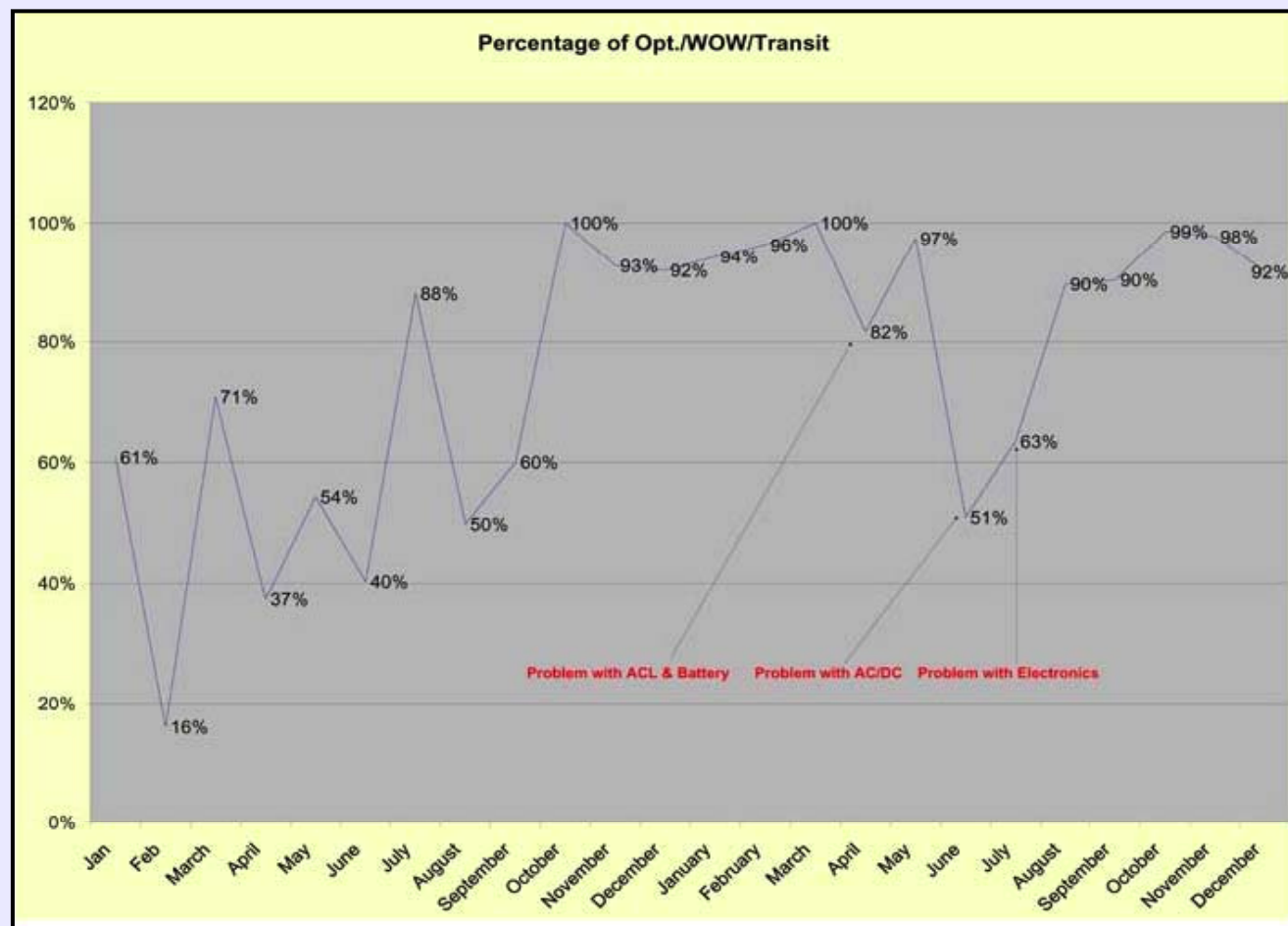


Risk Assessment and Risk Mitigation

Gwyn Griffiths

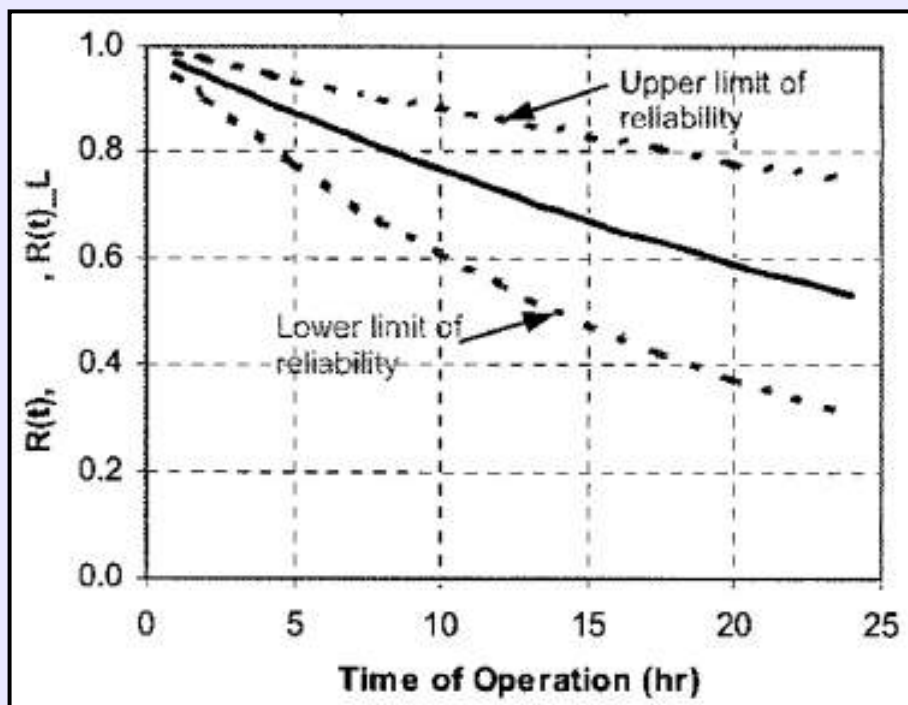


Availability of the C&C AUV 2001-2

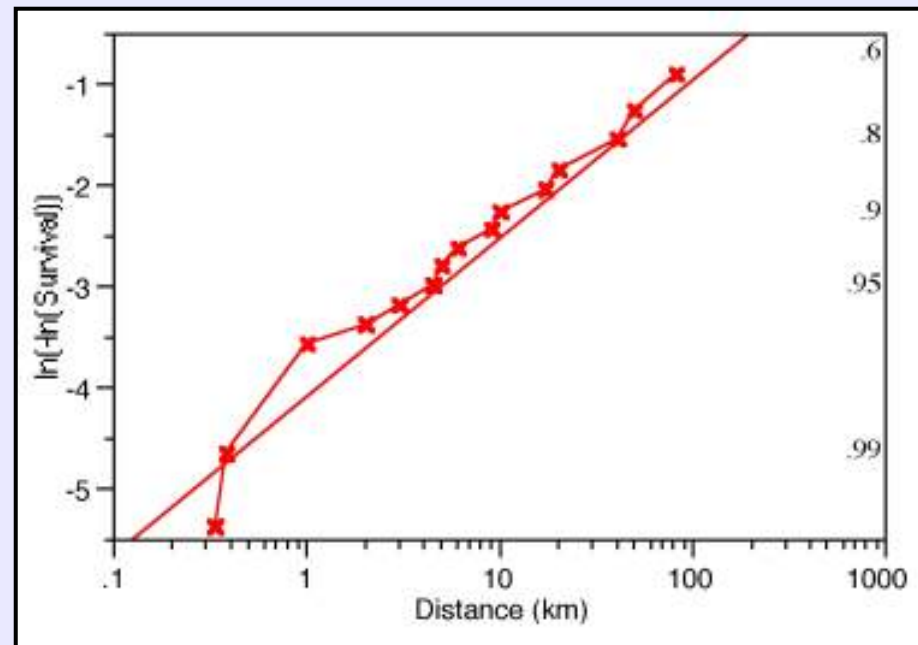


Percent availability for C&C Technologies AUV over 2 years and 24,000 km in the offshore industry. As delivered, availability was ~ 20%, but grew to 90-100% over a year of operations (from Chance, 2003).

Indicative reliability of two science AUVs



Probability of missions ending successfully (that is, without a fault causing premature termination) for the MBARI Dorado AUV, from Podder et al. (2004).



Probability plot for survival of Autosub, based on 240 past missions, with that estimated from a Weibull distribution with $\alpha = 403.9$ and $\beta = 0.678$. The right hand scale shows the probability of survival, from Griffiths et al. (2003).

Revealed vs Targeted Reliability

❑ Revealed Reliability

- No reliability goals
- Reliability issues inform decisions to some extent
e.g. Simplicity, Modular, use of standards, procedures, training ...
- Reliability presented as historical data, if at all

❑ Targeted Reliability

- Clear reliability goals within a Risk Management Process, that will include:
 - Risk identification
 - Assessment
 - Tests against risk acceptance criteria
 - Mitigation strategies

Provide assurance that designs can be achieved and information will be captured and analysed to show goals are being met.

Basic Risk Management Paradigm

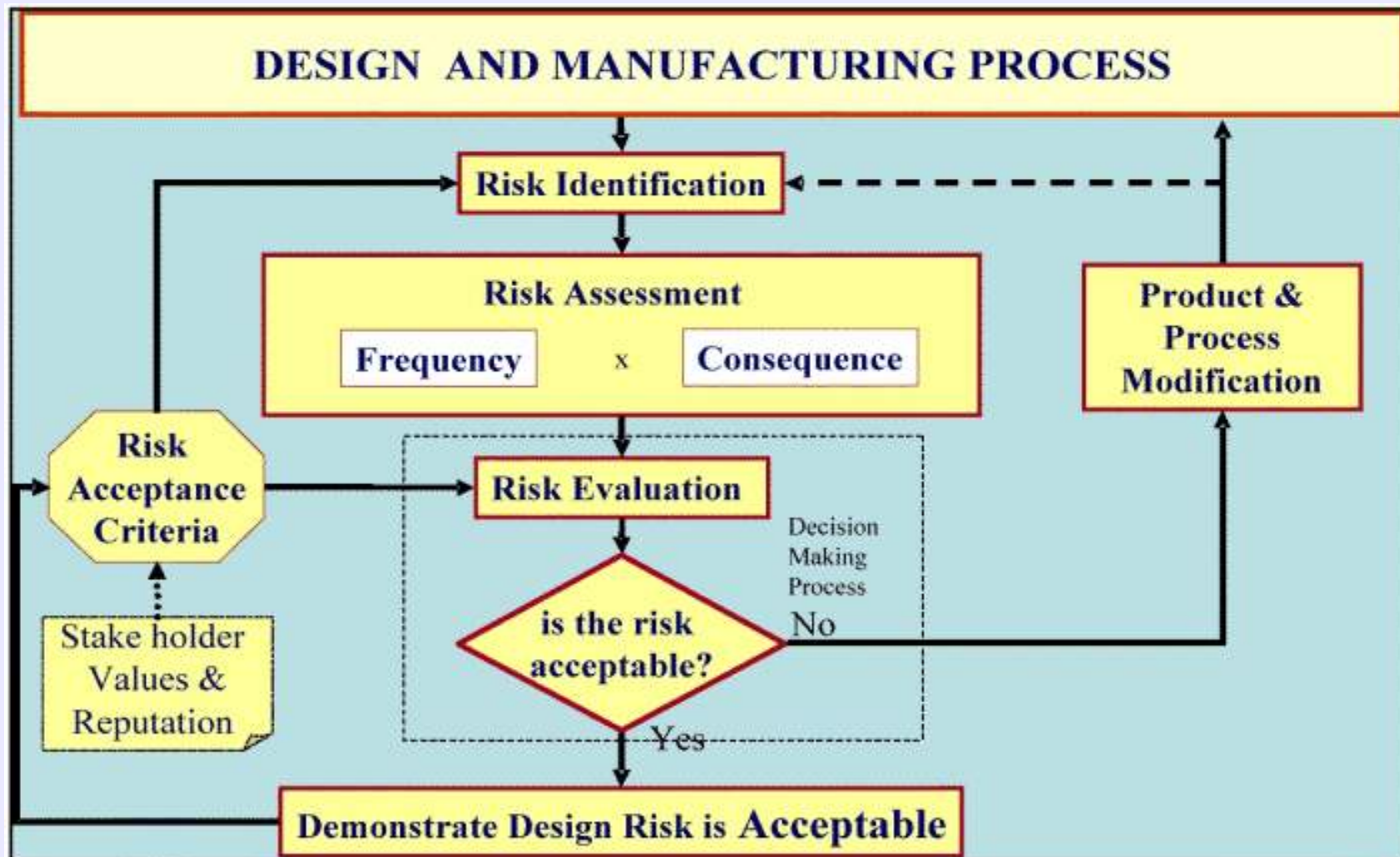
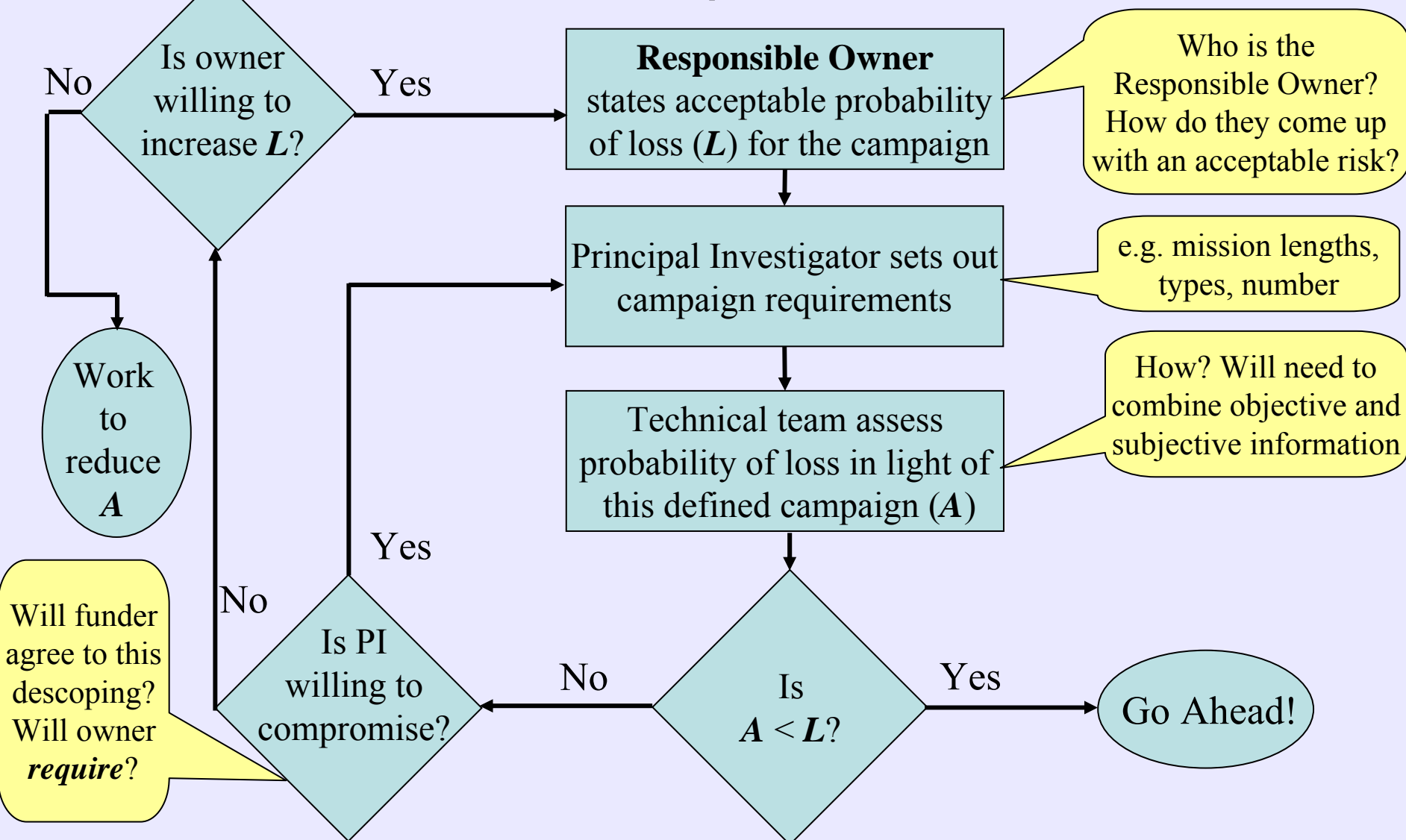


Diagram from Prof. J E Strutt, Boreas Consulting and Cranfield University



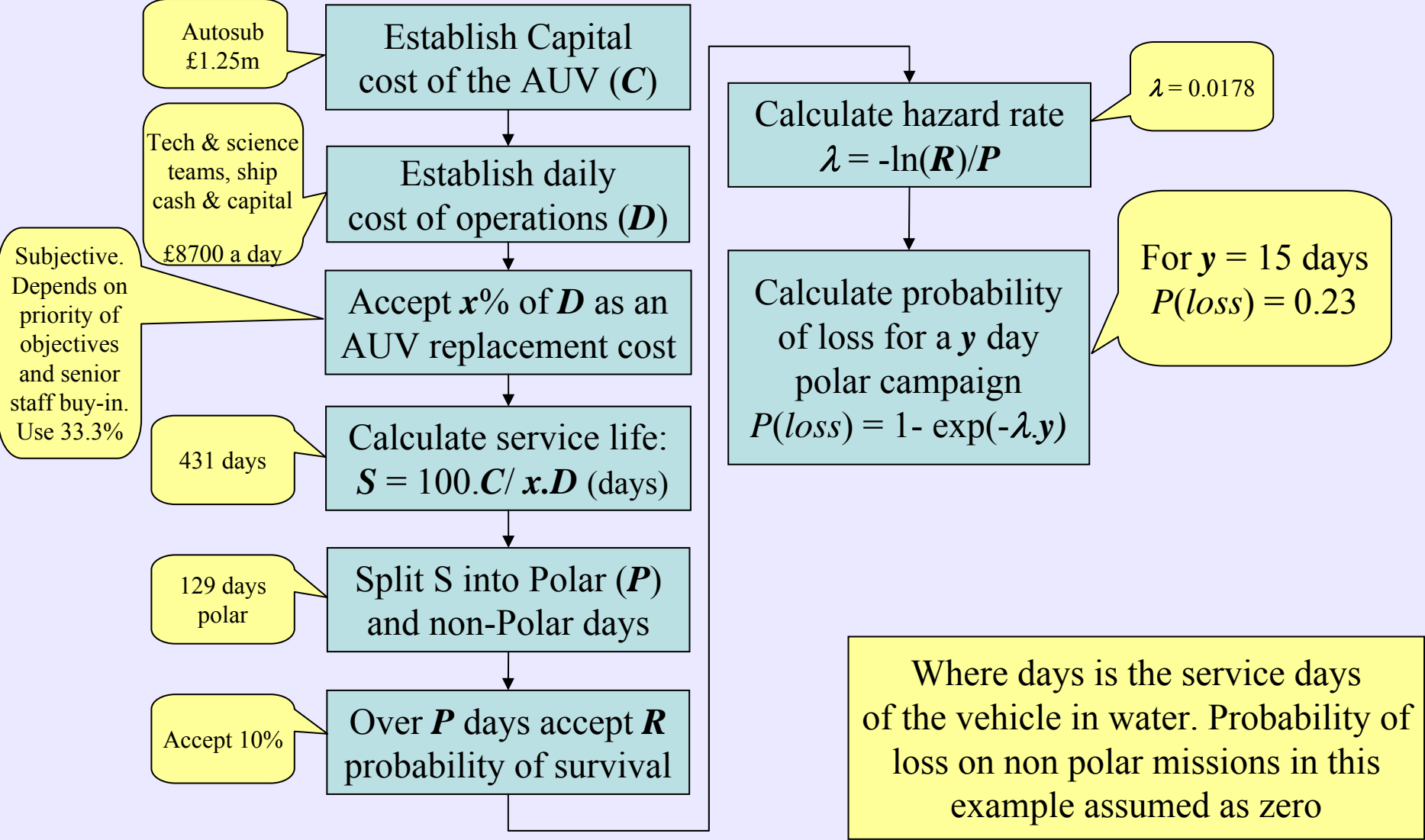
One Risk Acceptance Process



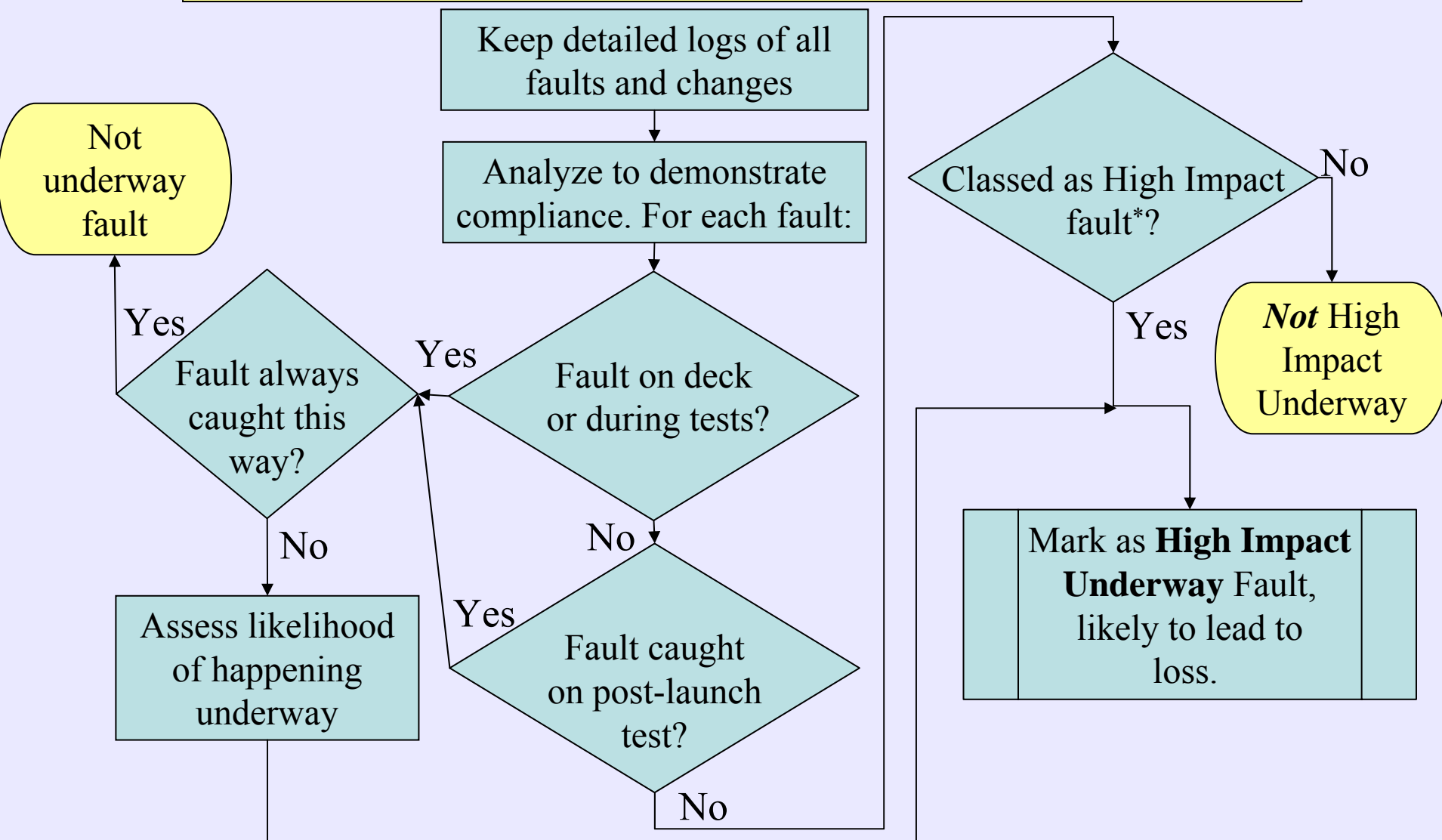
Who is the responsible owner?

- ❑ Exactly **who** may depend on level of risk
(*Commercial insurance unlikely to be obtainable or suitable if annual premium > 15–20% of value*).
- ❑ Some examples for a large, expensive AUV :
 - Over 50% probability of loss on one campaign:
Chief Executive, Chief Financial or Operating Officer
 - 20–50% probability of loss on one campaign:
Responsible Director
 - Less than 20%:
Head of the AUV facility

How *might* they come up with an acceptable risk?



Acceptable risk: Fault assessment



Acceptable risk: Calculation

1.

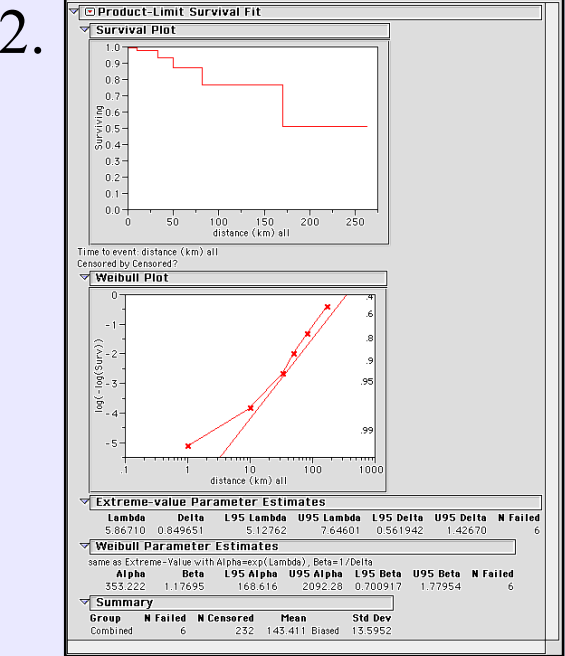
Mission	km	HI fault?
1	10	N
2	30	N
3	70	N
4	40	Y
5	80	N

3. Parameters of a Weibull distribution

Probability of Surviving distance x

$$R(x) = \exp\left(-\left(\frac{x}{\alpha}\right)^\beta\right)$$

α	β	L95 α	U95 α	L95 β	U95 β	N Fail	Censored
483	0.78	173	5105	0.46	1.16	9	109



4.

Mission	km	$R(x)$
101	10	0.952
102	50	0.842
103	140	0.682
104	140	0.682
105	140	0.682
480		0.254

5. Probability of loss is ~0.75 compared to an acceptable probability of 0.23. Reliability must be much improved.



Re-establishing reliability statistics

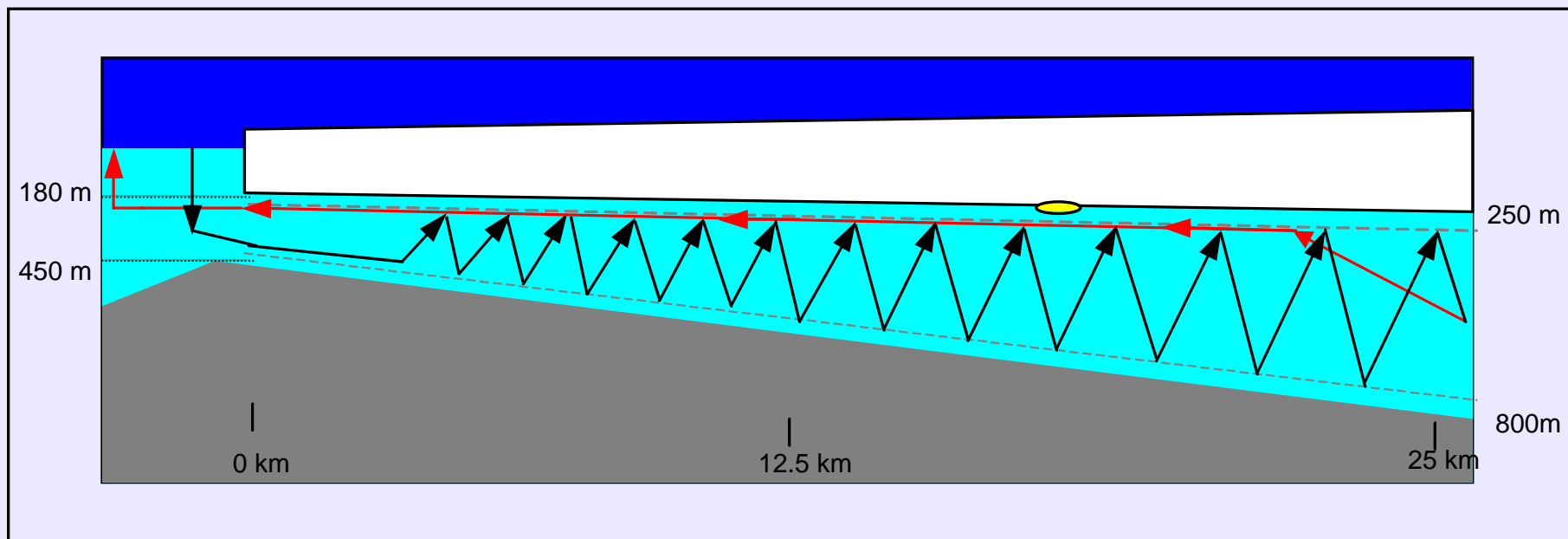
Mission (km)	1	2	3	4	5	6	7	8	9	10
Set	(km)	(km)	(km)	(km)	(km)	(km)	(km)	(km)	(km)	(km)
A	5 (F)	5	5	12 (F)	12	12	36	72	144	144
B	5 (F)	5	5	12 (F)	12	12	36(F)	72	144	144
C	5 (F)	5	5	12 (F)	12	12	36(F)	72	144	144*3
Weibull	Set	α	β	N_{fail}	N_{censor}	L95 α	U95 α	L95 β	U95 β	Time (days)
	A	632	0.54	2	8	74.7	7.5×10^8	0.11	1.36	7
	B	217	0.66	3	7	51.2	39223	0.20	1.41	7.25
	C	511	0.58	3	9	96.9	5.6×10^5	0.17	1.29	11

Three hypothetical scenarios for trials missions that set out to re-establish $\alpha > 480$. Upper part sets out mission lengths. An (F) indicates that a mission failed. The 10th mission in set C comprises three segments of 144 km each. Lower part shows the Weibull distribution parameters and an estimate of the time needed for the trials missions to be completed

Approaches to Mitigating Risk

- ❑ Adopt a Risk Management Process
- ❑ Procedural measures
 - Launch and recovery, training, communication
- ❑ Technical measures
 - Robustness, *prove* key components meet requirements
 - Determine most likely causes of failure
 - Design to avoid most likely causes giving rise to failure
 - Design trials to demonstrate achievement of reliability goals

Mission 383 Fimbul Ice Shelf, Antarctica



Has anyone seen our submarine?

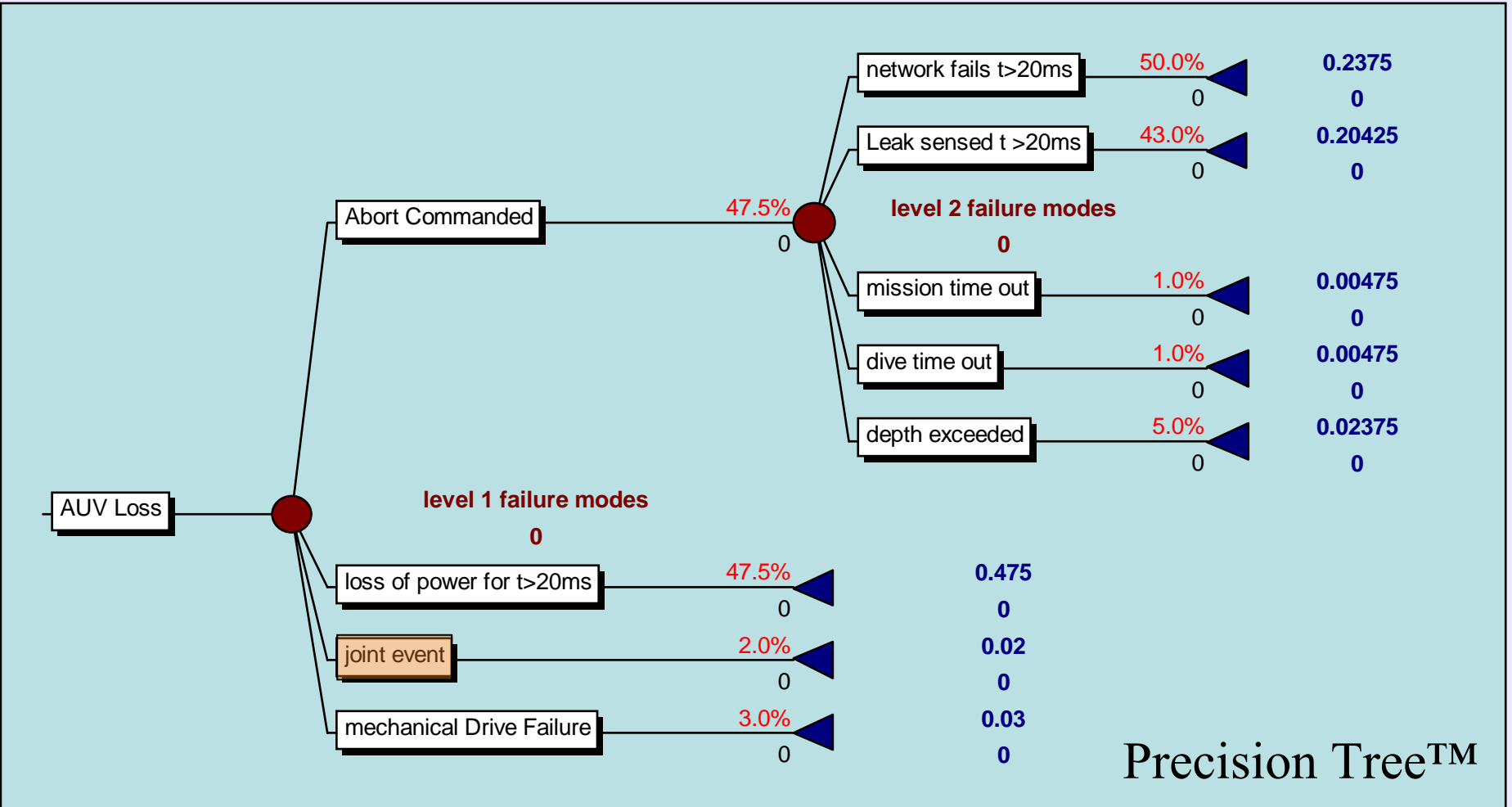
David Adam

Monday February 21, 2005

Lost: much loved robot submarine, last seen under 200 metres of Antarctic ice last Wednesday, answers to the name Autosub - reward.

The **Guardian**
UK news

Fault Tree Analysis



Precision Tree™

Diagram from Prof J E Strutt, Autosub Loss Inquiry Board



Major failure modes for Autosub

39 Major Failure Modes

AC: Abort Commanded

LP: Loss of Power

JE: Joint Event

MF: Mechanical
Failure

CAT	N	Failure Mode	Probability
AC	1	NetX in dry domain fails	0.0855
AC	2	NetY in dry domain fails	0.0475
AC	3	NetY in wet domain fails	0.0475
AC	4	DGO connector failure	0.0460
AC	5	harness joint failure	0.0409
AC	6	Endcap seal failure	0.0383
AC	7	Burton connector failure	0.0306
AC	8	bulkhead connection (netX) fails	0.0285
AC	9	harness failure (netX wet)	0.0285
AC	10	depth exceeded	0.0238
AC	11	Leakage thru bonding on transition ring	0.0153
AC	12	Connector plug failure	0.0153
AC	13	Sensor failure	0.0102
AC	14	Internal Condensation	0.0077
AC	15	Mission time out	0.0048
AC	16	dive time out	0.0048
LP	17	pcb wiring failure	0.0475
LP	18	current sensing resistor failure	0.0475
LP	19	Inrush current protector	0.0475
LP	20	dc-dc converter (fused)	0.0475
LP	21	magswitch failure	0.0475
LP	22	main power switch failure	0.0475
LP	23	Motor controller fails	0.0380
LP	24	short circuit on harness	0.0380
LP	25	fuse pot fails	0.0214
LP	26	Net X fails in dry domain	0.0171
LP	27	Short on wires in maintenance	0.0143
LP	28	bulkhead connection (netX) fails	0.0128
LP	29	harness failure (netX wet)	0.0128
LP	30	battery exhausted thru high current demand	0.0119
LP	31	fuse and diode fail	0.0071
LP	32	calculation error in battery life	0.0048
LP	33	dc-dc converter failure	0.0048
LP	34	harness connector fails in dry domain (low resistance path)	0.0036
LP	35	harness connector fails in wet domain (low resistance path)	0.0036
JE	36	unusual terrain impact	0.002
JE	37	AUV control failure and Impact together	0.018
MF	38	loss of mechanical drive	0.015
MF	39	drive jammed	0.015
TOTAL			1.000

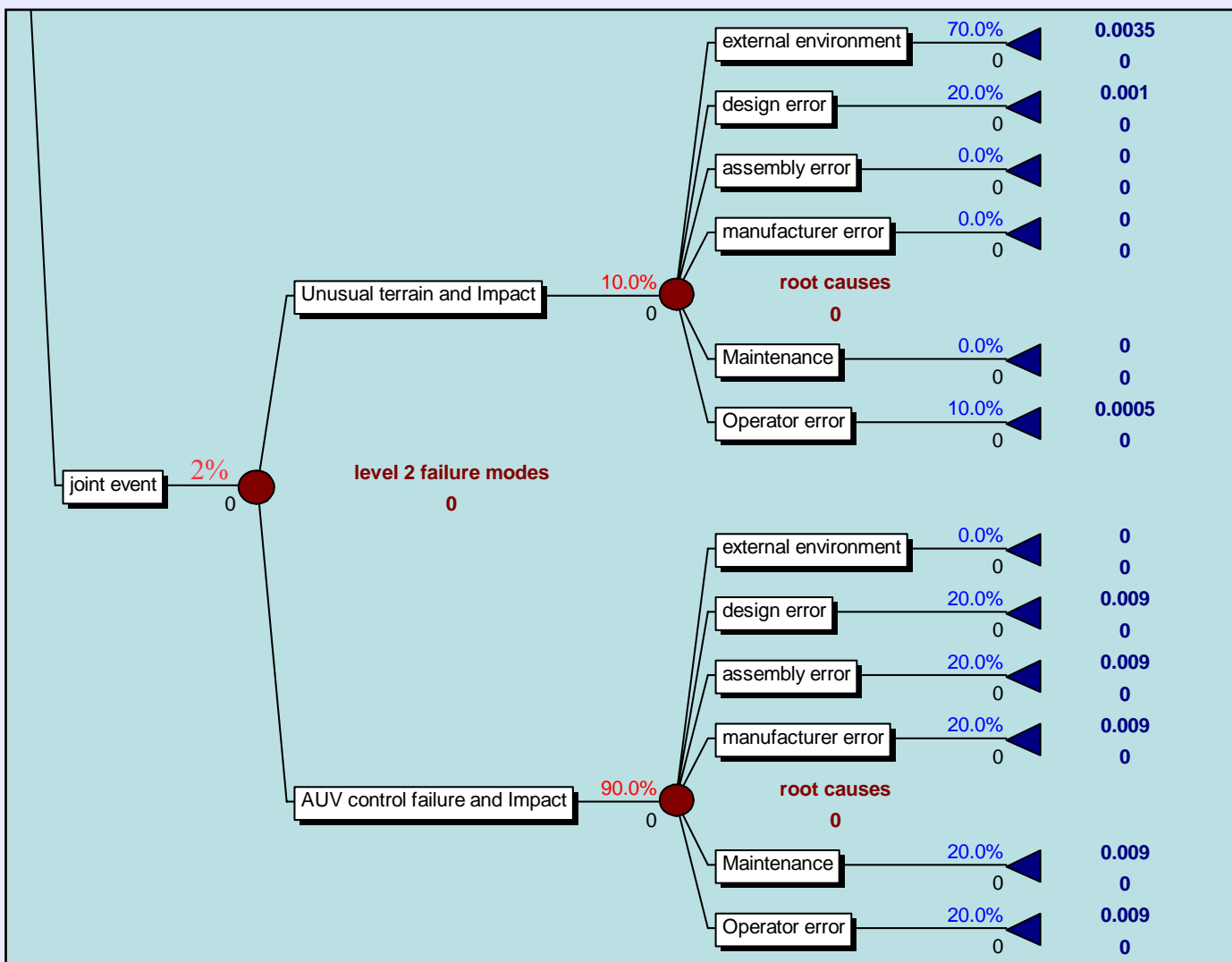
Summed to give

Summed to give

From Prof J E Strutt
Autosub Loss Inquiry Board



Root Cause Analysis



Errors in:

- ⇒ Design
 - ⇒ Assembly
 - ⇒ Manufacturing
 - ⇒ Maintenance
 - ⇒ Operator
- or due to the*
- ⇒ External environment

From Prof J E Strutt
Autosub Loss Inquiry

References

- Chance, T. S., 2003. AUV surveys – extending our reach, 24000 km later. Proc. UUST 2003, AUSI, New Hampshire.
- Griffiths, G., Millard, N. W., McPhail, S. D., Stevenson, P. and Challenor, P. G., 2003(a). On the Reliability of the Autosub Autonomous Underwater Vehicle. *Underwater Technology* 25(4): 175-184.
- Griffiths, G., Millard, N. W., McPhail, S. D. and Riggs, J., 2003b. Effect of upgrades on the reliability of the Autosub AUV. Proc. UUST 2003, AUSI, New Hampshire.
- Podder, K., Sibenac, M., Thomas, H., Kirkwood, W. and Bellingham, J., 2004. Reliability growth of Autonomous Underwater Vehicle – Dorado. Proc. Oceans 2004, Kobe, Japan. MTS/IEEE. Pp. 856-862.
- Stokey, R., Austin, T., von Alt, C., Purcell, M., Goldsborough, R., Forrester, N. and Allen, B., 1999. AUV bloopers or why Murphy must have been an optimist. *Proc 11th International Symposium on Unmanned Untethered Submersible Technology*, New Hampshire, AUSI, pp. 32-40.
- Strutt, J. E. et al., Report of the Autosub Loss Inquiry 2005. To be available from NERC and NOCS in due course.

