SAFETY INTEGRITY LEVEL ASSESSMENT FOR DIVING REBREATERS AND ASSOCIATED EQUIPMENT

DOCUMENT: SA_SIL_Assessment_100625.doc

ORIGINATOR: **Dr. Alex Deas, Dr. Vladimir Komarov, Igor Abrosimov, Dr. Sergei Pyko, Dr. Sergei Malyutin, Dr. Bob Davidov**

DEPARTMENT: **Engineering**

DATE UPDATED: **25th June 2010**

REVISION: **B3**

APPROVALS	
_____IA_____ Hardware Architect	___**25th June 2010**_____ Date
_____ SM_____ Software Architect	___**25th June 2010**_____ Date
_____AD_____ Project Manager	___**25th June 2010**_____ Date
_____VK_____ Quality Officer	___**25th June 2010**_____ Date

Controlled Document ☒ Classified Document ☐ **DO NOT COPY.**

Revision History

Revision	Date	Description
A1-3	8th March 2007	A1 (8 March 207): SIL Assessment Finalisation for Open Revolution Submission. A2 (12th March 2007) Reviewed, with hyperbaric manning feedback. A3 (20th Aug 2007): UK HSE SIL Assessment method comparison
B1	12th May 2008	Correction of revision, minor typos. Addition of mCCRs.
B2	24th Dec 2008	B2: 18th Dec 08, Updates arising from EN61508 audit review of SIL. B2R: 24th Dec 08Proof read and approved for release as B2R. Title updated.
B3	25th June 2010	Updated risk tables. Updated references to certification.

Table of Contents

1. PURPOSE AND SCOPE

This document provides the Safety Integrity Level Assessment of diving equipment forming the Open Revolution Project Submission by Deep Life Ltd.

The identity of the appropriate SIL requirement is generic and believed to apply to all eCCR and eSCRs, PPO2 monitors and diving comms packages.

This assessment was performed in compliance with EN61508:2004 and Deep Life Quality Procedure QP-23. The latter procedure is part of a process that has been certified to comply with EN 61508.

The equipment being assessed is:

- Incursion eCCR for military diving applications
- Bell diver's eSCR for commercial (umbilical) diving
- Apocalypse mCCR for sports diving with PPO2 and PPCO2 monitors
- Hyperbaric controller using Bell Diver's rebreather core as the primary controller
- Optional commercial diving package of multiplexer (MUX) with Topside Termination Unit for the umbilical
- Optional Topside Software

2. METHOD

The method of calculating a Safety Integrity Level is stipulated in Quality Procedure QP-23. The relevant section of that procedure is reproduced below, along with its reference to the Table 22.2 in QP22.

2.1. SIL is based first on Risk, not Consequence

The assignment of SIL level is based on the cost of risk, derived from the probability of each mode failure and its consequence. That is, the process of assigning a Safety Integrity Level, does not search for the worst possible consequence of a failure. It identifies what the risk is, and assigns a cost of that risk based on how probable the event is.

COST	SIL	High demand rate (maximum failures per hour permitted)	Low demand rate (maximum failures per demand permitted)
< 4	No SIL	Not defined	Not defined
>= 4	0+	10^{-5} to 10^{-4}	10^{-2} to 10^{-1}
>= 8	1	10^{-6} to 10^{-5}	10^{-2} to 10^{-1}
>= 16	2	10^{-7} to 10^{-6}	10^{-3} to 10^{-2}
>= 32	3	10^{-8} to 10^{-7}	10^{-4} to 10^{-3}
>= 64	4	10^{-9} to 10^{-8}	10^{-5} to 10^{-4}
>= 128	4+	< 10^{-9}	< 10^{-5}

Table 23.1: Assigning SIL reliability targets based on the cost of the risk.

2.2. SIL Assignment Process

The process of assigning a Safety Integrity Level to a piece of equipment or a process has the following steps.

1. Perform a Fault Tree Analysis (FTA) of the equipment or the process. To build the FTA, follow the procedures in QP-20 and QP-21 (Accident Studies, HAZIDs, HAZOPs, Failure Analysis, FMECA development).
2. Using the FTA, apply a risk assessment according to QP-22 Section 22.8, to determine the risks associated with the activity under review and their consequence, should the function being designed or considered fail, for each of the terminal cases identified in the FTA. The Safe Failure Fraction is core to this assessment.
3. Use Table 22.2 in QP-22, to relate the risk and its consequence to a cost. The cost is in brackets in Table 22.2. For example, the risk of a severe failure defined in Table 22.2 occurring less than once in a billion hours, is cost (8).
4. Take the highest cost and look up the SIL rating using Table 22.2.
5. Benchmark the SIL assignment using both pragmatic and controllability approaches in accord with current UK HSE guidelines.
6. Review the ethical acceptability of the risks, with comparison to common documented risks and benefits of the proposed activity.
7. Record the calculation in the current Colour Book and ensure all involved on the project are aware of the SIL rating.

<Remainder of page blank>

POTENTIAL SEVERITY CRITERIA				PROBABILITY/POTENTIAL FOR EVENT OCURRENCE				
Given a random set of circumstances, what is the worst event that could happen?				A VERY UNLIKELY	B UNLIKELY	C POSSIBLE	D LIKELY	E VERY LIKELY
DESCRIPTION	HARM TO PEOPLE	ENVIRONMENT	DAMAGE	Less than once per billion hours	Less than once per ten million hours	More often than once in ten million hours	More often than once in 100k hours	More often than once in 1000 hours
5 CATASTROPHIC	More than 20 Fatalities / Multiple Serious Injuries. Likely to prevent operational Safety Case acceptance	Massive & uncontrolled release with significant environmental impact extending well beyond site boundary. Chronic pollution resulting in damage lasting more than 12 months.	Over €5,000,000	5A (32)	5B (64)	5C (64)	5D (128)	5E (256)
4 SEVERE	Up to 20 individual Fatalities or Serious Injuries. Injury resulting in permanent and severe disability. May prevent Operational Safety Case acceptance	Extended breach of licence conditions & / or uncontrolled release. Significant environmental impact beyond the site boundary unlikely to last beyond 12 months. Recovery/rehabilitation requires external assistance	More than €50,000 less than €5,000,000.	4A (8)	4B (16)	4C (32)	4D (64)	4E (128)
3 SIGNIFICANT	Temporary or permanent partial disability.	Outside the site boundary. Localised pollution giving rise to significant environmental impact but unlikely to last beyond 1 month. Repeated breach of licence conditions. Recovery/rehabilitation may require external assistance.	More than €10,000, less than €50,000	3A (4)	3B (8)	3C (16)	3D (32)	3E (64)
2 MODERATE	Day Away From Work case (DAFWC) Medical Treatment / Restricted Work Case	Within site boundary. Short term environmental impact. Single licence breach recoverable by worksite.	More than €1,000, less than €10,000	2A (2)	2B (4)	2C (8)	2D (16)	2E (32)
1 NEGLIGIBLE	First Aid Injury	Within site boundary. No significant environmental impact or breach of licence conditions. Easily controlled / recovered by worksite	Less than €1,000	1A (1)	1B (2)	1C (4)	1D (8)	1E (16)
Scores in boxes (in parenthesis) may be used for statistical purposes to assess total incident risk-cost product.				MAPPING RISK COST TO SIL ASSIGNMENT TO MANAGE THE RISK: Untenable >=(128) SIL 4 >=(64), SIL 3 >= (32) , SIL 2 >= (16), SIL 1 >= (8), No SIL < (8)				

Table 1: Risk cost from Table 22.2 of QP22. Note that cost increases with risk are not linear between Severe and Catastrophic because to societal acceptance of air accidents, pharmaceuticals, major pollution incidents and of aspects of war. Any rating depending on a cost 5C or 4D needs special care to ensure it is a SIL 4 risk, rather than untenable risk.

3. SIL CALCULATION FOR ECCR AND ESCR

3.1. Fault Tree Analysis (FTA) Review

The FTA reviewed was a substantial document: 52 sheets, and forms FMECA 7 for the equipment. The same data is contained in Volume 6 in the form of HAZOP results and a HAZID walkthrough.

3.2. Risk Assessment

The risk assessment was carried out in accord with Quality Procedure QP-22, and mapped to the Risk & Consequence Table 22.2, reproduced above. This is a formal method of Safety Integrity Level assessment based on risk inherent with the operation and the reduction in risk required from the safety system.

From the FTA, it is clear that the equipment must operate continuously to maintain the life of the user. Numerous failure modes would result in a critical failure, where the unit is not injecting the correct quantity of oxygen, or it allows the CO2 levels to rise sufficiently to cause unconsciousness and death.

Where the equipment is used as a hyperbaric monitor and PPO2 controller, the lives of up to 18 divers could depend on the system. This may increase to 24 in the new generation of habitats. The equipment is used almost continuously in this application but double checks are made as to the mix gas and pressures. **This assessment would put the risk-cost as per Table QP22.2, at Likely Severe to Catastrophic-, a risk-cost of 128.**

Five hundred units of the equipment in the eSCR configuration for commercial diving are expected to be in use within five years. Each unit will be used for 80 hours per month, which is 40,000 hours. A failure to achieve the design intent would be a critical failure but should be noticed by the Dive Supervisor and bail out onto umbilical gas. The failure would likely cause grounding of the equipment and possibly the fleet. Any critical failure would likely cause suspension of the product at a cost well in excess of €500,000. **This assessment would put the risk-cost as per Table QP22.2, at Likely Severe to Catastrophic, a risk-cost of 128.**

The equipment is expected to be produced in large volumes for sports divers with targets of well over 1,000 units in active use, with a medium annual usage of 40 hours each. That is, 40,000 hours per year in active use.

The review of contemporary equipment which it replaces, is that without monitoring the unit will have a critical failure around once in 5,000 hours with 1 in 4 of these being survived by the wits of the diver. This figure is based on the APD Inspiration. It would mean that for each 1000 units in use in the Sports market, 2 divers would have a fatal accident per annum. For the seven service year life of the equipment this would be 14 fatal accidents per 1000 units. **This assessment would put the risk-cost as per Table QP22.2, at Likely Severe, that is, a cost of 64.**

Using Table 23.1 in QP-23, all applications of the equipment put the SIL rating at Category 4.

4. SIL CALCULATION FOR MCCR

4.1. Fault Tree Analysis (FTA) Review

The same FTA is used as for the eCCRs, but with special consideration of mortality statistics for mCCRs since their introduction.

4.2. Risk Assessment

The risk assessment was carried out in accord with Quality Procedure QP-22, and mapped to the Risk & Consequence Table 22.2.

The risks are the same as for the eCCR, except that continuous intervention is required by the diver. The mCCR has a means to ensure the diver does carry out this interaction, and bails out the diver onto open circuit where the interaction does not occur with sufficient frequency.

Cost of a mortality depends on the societal acceptance of the risk. Society accepts that the risk involved in diving is higher than that in a normal office environment, and therefore that sports divers are risk takers. The SIL assessment looked for numerical data on which to obtain an objective cost to that societal risk.

There is data on the cost of a sports diving rebreather fatal accident from the legal cost of eCCRs sold into the same market, i.e. to sports divers since 1998. The leading company in this market has sold 2,700 of their first eCCR product, and 68 diver mortalities have been identified for that product – the actual number is likely to be higher as the type of equipment is not known for all diving fatal accidents that have occurred. This equates to one mortality per 39 units sold. There are features of that product that are likely to give rise to a significantly higher mortality rate and a higher legal cost than is expected for the Open Revolution mCCRs per unit[1]. The total legal cost of €600k for that company seems to appear as a "management charge" in the public accounts of the company. This equates to €8,800 for each diver mortality.

This cost figure of €8,800 per mortality is very low, probably unethically so. In process industries figures of €2mn to €3mn per mortality are normal, and in the nuclear industry figures of up to €200mn are used. The €8,800 figure determined from the historical cost of eCCR sports fatalities, equates to Moderate cost in Table 22.2: the same as a day off work in Table 22.2, would the cost matrix would equate that to SIL 0 to SIL 1. Given the nature of the equipment, such a low rating is unreasonable: the cost needs to be adjusted for the cost of a claimant succeeding following a mortality. This cost is likely to be two claimants out of the 68 mortalities claiming €3mn each, based on mortality cost assignment in the process

[1] The cost of sports diver mortalities is based on an analysis around the Inspiration and Evolution rebreathers, developed and sold by Ambient Pressure Valves (Parker Diving Ltd) and Ambient Pressure Diving Ltd, from 1998 to 2008. It is represented that the use of these benchmarks provides a worst case because the Inspiration and Evolution were not been developed to any recognised Functional Safety standard and the developers were incompetent: the Project Leader for the Inspiration (Martin Parker) had no higher education, nor any experience in complex design that is implicit for a rebreather, and the designer of the Inspiration electronics and software (Nigel Hester) admitted to have no engineering qualifications whatsoever. As a result of this lack of competence, the Inspiration and Evolution products were not properly verified before sale and had numerous basic design mistakes allowing units to hang, reset and otherwise fail to carry out basic safety functions. No recognised safety architecture was used, such as TTA. The Inspiration and Evolution equipment did obtain a PPE Certification but do not comply with the relevant harmonised PPE standard, EN14143:2003, on numerous grounds (markings on the equipment claiming compliance are fraudulent). That PPE certificate has been effective in providing protection from prosecution in Europe – coroners assume it implies that the equipment implements best practice, and the certification encouraged public safety organisations to turn a blind eye to the safety issues. The extremely high mortality risk per unit was hidden by exaggerated sales figures being circulated, and measures being taken to prevent discovery of the actual sales figures. Divers in the USA sign numerous liability waivers in their training, which has so far afforded APD a degree of legal protection in cases in the USA. Taking this equipment as the basis for the analysis of cost per mortality is therefore appropriate (as the Open Revolution will also be PPE Compliant, and uses legal waivers in North America), but is worst case, as the Open Revolution units have been designed competently, by engineers meeting all qualification and experience requirements, following a certified IEC EN 61508 process, which should reduce the mortality rate greatly and provide a basis for lower costs of legal defence compared with a non-compliant product.

industry. On the basis of two claims succeeding, this would equate to a cost per mortality of around 2*€3mn/68, or €88k. **This would equate with a Severe cost in Table 22.2, and a risk-cost of 32 to 64 in Table 23, which is a SIL 3 assessment.**

The approach taken in the mCCR is to provide multiple independent monitors, of different operating principle. Due to the redundancy and diversity, the implementation of each monitor would require to be SIL 2.

5. SIL CALCULATION FOR MUX AND TERMINATOR

Moving to the multiplexer and communications for the commercial eSCR, the FTA shows that the failure of this would cause the dive to be aborted, and a new dive arranged an hour or so later when replacement equipment is provided.

The cost of an oil well servicer vessel is put at €150,000 per day, or €6,250 per hour. **This would be a risk-cost for the MUX and Topside Unit of 16 in Table 22.2, which equates to SIL 2 using Table 23.1**

6. SIL CALCULATION FOR TOPSIDE SOFTWARE

Loss of the software would not cause a recall of the diver: it is multi-entry using Python to run from any web browser. The software would have an inconvenience level to restart, and would cause the loss of under €1,000 on malfunction. The eSCR does not permit the software to bring the equipment outside the safety envelope for the diver.

The cost of an oil well servicer vessel is put at €150,000 per day, which for a system reset is a cost of 8 for the software, which equates to SIL 1 in Table 23.1. **If two versions of the system were running, the system would be SIL 0 but the review here declines to assign SIL 0 due the overall safety nature of the system and assigns SIL 1.**

7. SIL CALCULATION FOR PPO2 MONITOR

The PPO2 monitor may be used on the eCCR or as a PPO2 monitor on a mCCR. The number of units in the later configuration would be 500 or less.

The FTA for the PPO2 Monitor is identifies the following risks:

- In a mCCR it would be apparent the unit has failed because the diver is injecting oxygen manually and looking for the response from the monitor. The risk of a fatal accident from a failure is therefore low, but is plausible. The likely outcome, defined in terms of Table 22.2 from QP22, is of an increased risk of De-Compression Syndrome, that is, of temporary or permanent disability.
- In the eCCR the monitor is a low usage system, in that it acts as a monitor for the PPO2 monitor integrated into the eCCR.
- It is not envisaged the monitor be used with the rebreather in the eSCR configuration, but if it is, then the case is the same as for the eCCR.

This assessment would put the risk-cost as per Table QP22.2, at Possible Significant, that is, a cost of between 8 and 16, which equates to SIL 2 for any individual module, where several diverse modules work together to perform a SIL 3 role.

8. RISK REDUCTION FROM SAFETY SYSTEM

The Open Revolution equipment of which this document forms part of the safety case, is designed to achieve a MTBCF of better than 1 in a billion hours. This moves the risk from

128 to a Very Unlikely Severe Risk, Cost 8 in Table 22.2. This is the same risk-cost as a First Aid injury every 10k to 100k hours, or a financial loss of €1,000.

For the optional monitors and comms, the use of the system reduces the risk-cost by the quad root, so a risk-cost of 16 reduces to 2, and 8 reduces to 1.7.

9. APPLICATION OF ALARP

The equipment can be designed to achieve SIL 3 to 4 MTBCFs within both practical and economical bounds.

The Achilles heel of these products is the lack of diversity in the oxygen sensors: all are the same type. Efforts to increase diversity have been applied, including:

1. Use of sensors from different batches.
2. Efforts to approve sensors from more than one manufacturer, and use of sensors from more than one manufacturer in each product.
3. Oxygen sensors are read by different ADCs, so a catastrophic failure of one does not affect any other sensor reading: the common mode ADC failure is mitigated.
4. A diversity of implementation is used in the electronics that reads the sensors (FPGA and verified MCU), or in the case of the mCCR O2 pods using different MCU implementations to monitor O2 measurements and their reporting.

This limited diversity of oxygen sensor type is the limiting factor in the safety case, but ALARP has been applied vigorously.

DL use oxygen sensors from different batches, and endeavour to qualify two manufacturers, but all sensors are of the same type: galvanic oxygen sensors. It is highly desirable for a second technology to be used alongside the galvanic sensors to remove common failure modes. After the sensors, DL's Open Revolution rebreathers have diversity as well as redundancy: use of two completely different technologies for processing the O2 data. It is recognised that the present approach applies ALARP, as it is not practical to install a mass spectrometer in a rebreather as an alternative oxygen measurement technique, and Sol-gel sensors are not operating reliably at the present time with oxygen pressures above one atmosphere

The diversity issue is managed in the case of carbon dioxide sensing, by use of consistent scrubbers that are well characterised, a carbon dioxide sensor and the diver's own symptomatic feedback from the onset of hypercapnia. In the eCCRs, scrubber health monitoring and scrubber endurance prediction are also provided.

A full safety case is made for the equipment commensurate with the SIL 4 rating of the system for the eSCR and eCCR. However, there is an intellectual barrier in assigning such a high SIL rating to a self contained piece of equipment, and a SIL 3 assignment would be the maximum that can be justified. The SIL 4 assignment therefore should imply that the project use SIL 4 rigour in managing the life cycle of the equipment, but the equipment itself would be SIL 3 if the design process meets all the EN61508 and CASS requirements for at least SIL 3.

The intellectual bridge from SIL 3 as a formal assessment to SIL 4, would require a diversity of method used to measure the PPO2: use of different sensor types, such as multiple galvanic sensors and mass spectrometry – this is not feasible at this time on a piece of diving equipment.

The MUX and comms package for the eSCR is assessed at SIL 2, which means that dual redundancy is required.

The SIL 1 rating for the topside control software can be achieved by the provision of multiple copies running on different platforms. This capability is intrinsic to the design, using the Python language. In the worst case, the whole system can be controlled via a Python capable mobile telephone.

10. BENCHMARK CHECKS

There appears to be no catalogue available of comparable equipment, which can be used as benchmarks for the SIL assignment. However, the UK Health and Safety Executive have considered the methods for SIL assignment carefully and have published guidance on this, which is relevant to the equipment under consideration. The two most important of these reports are referred to below.

10.1. UK HSE SIL Assignment Method

The UK Health and Safety Executive Research Report 216[i] provides an excellent overview of the standards, consideration of the assumptions implicit to the SIL assignment and their role in risk assessment. The report had a specific focus on IEC 61508, so has a special relevance to this study.

The report considers Pragmatic, Controllability and Standards based approaches to SIL assessment.

10.1.1. Pragmatic Approach

The HSE Research Report 216 refers to the MISRA method developed by the automotive industry. This is particularly relevant here because a single accident will usually result in one or two deaths in the worst case, but the product is produced in volume so one fault can cause large numbers of accidents. The MISRA SIL rating differs from the EN61508 ratings n that they move down one step, namely MISRA SIL ratings are:

> **SIL 1** - represents the integrity required to avoid relatively minor incidents and is likely to be satisfied by a certain degree of fault tolerant design using guidelines that follow good practice.
> **SIL 2** - represents the integrity to avoid more serious, but limited, incidents some of which may result in serious injury or death to one or more persons.
> **SIL 3** - represents the integrity required to avoid serious incidents involving a number of fatalities and/or serious injuries.
>
> **SIL 4** - represents the integrity level required to avoid disastrous accidents.

A design fault that causes a fatal accident, in a mass produced product, would be SIL 3. A fault where many people could be put at risk is SIL 4, such as a toxic gas tanker leaking in a city. This appears to be a down rating of the EN61508 SIL assignments simply because there is a higher public acceptance of risk from automotive transport than for less necessary equipment. This is the societal cost that was also considered for the rebreather case.

The EN61508 SIL ratings apply to generally acceptable levels for risk, where a member of the public should an activity to have a risk less than one fatality per 10^6 years of equipment operation, per item of equipment, and allow risks to increase by an order of magnitude for each reduction in the consequences of a failure of the equipment. Hence, EN61508 SIL assignments are as follows:

> **SIL 1** is the level required to avoid serious accidents
>
> **SIL 2** is the level required to avoid multiple serious accidents, which alone are not likely to be fatal.
>
> **SIL 3** is the level required to avoid fatal accidents

SIL 4. Is the level required to avoid accidents of 20 or more people

EN61508 was not developed with mass production in mind, where there are tens of thousands of life critical systems in use. The ethical issues of this were considered at length, and the conclusion was that a single fault that can cause 20 deaths spread over the operating life of the equipment deserves the same SIL rating as a single fault that can cause 20 deaths at one time. The reasons for this are:

1. The cost to the equipment manufacturer will be higher in the case of 20 individual accidents, than one large accident, as there will be 20 legal cases to defend.
2. The cost to society in the case of 20 individual accidents is the same as for one large accident.
3. The damage to the reputation of the manufacturer is likely to be the same or higher if there is a string of fatal accidents, or one accident.
4. The political damage caused by one large accident is not considered: the politics of the country should be irrelevant to safety assessment.

In this pragmatic assessment, comparison was made with equipment that was involved in the most serious accidents. It is noted that the MISRA listing does NOT condone processes and equipment which are simply not ethically acceptable: the MISRA rating applies to motor vehicles where generally one accident kills one person. Accidents where one fault can kill many abound, but most of them fall outside any ethical SIL assignment.

10.1.2. The pragmatic distinction between SIL 3 and SIL 4

There is an intellectual barrier to assigning SIL 4 to any self contained equipment because:

1. Major facilities such as civil nuclear reactors struggle to meet SIL 4 requirements. The safety audit for a nuclear reactor takes typically 50 to 100 man years, and the team look for both redundancy and a diversity of safety systems. In a rebreather diversity of oxygen sensors is hard to achieve, other than using oxygen sensors from different batches and different manufacturers. The safety audit for the rebreather by contrast is just 20 to 25 man years (including verification), and the formal EN61508 audit of that is just six man weeks.
2. Civil aircraft fail to achieve SIL 4: for example, the controllers for active wing surfaces only achieve SIL 3. The verification and audit of the rebreather controllers is comparable in scope with that of civil aircraft active surface control hardware: SIL 3 is appropriate because passengers in an aircraft do not have a bail out, but divers do. This presence of bail out means that divers should be exposed to less risk, therefore not as high a SIL, as that of passengers on a civil airliner.
3. SIL 4 and its North American equivalent has used to justify plants that are simply beyond any ethical justification. A good example is the Union Carbide accident in Bhopal in 1984.

The Union Carbide Bhopal plant made a pesticide called Sevin, the production of which involved the production of Methyl Isocyanate (MIC), an extremely toxic gas that had to be kept free from contaminants and below 0C to avoid an uncontrolled reaction in which it breaks down to form cyanide compounds. Union Carbide decided to allow 200 tons of this MIC to be stored in a plant in a highly populated city – Bopal, in India, and did not disclose the cyanide products. When the plant was operated by the engineers who designed it, there were few accidents (but there was a fatal accident from phosgene, used in the manufacture of MIC). The management of Union Carbide decided to shut down the plant for economic reasons. All the safety systems were switched off: all monitors on the MIC were off or known to be out of order, the flare to burn off any accidental releases was switched off, the cooling for the MIC tanks was switched off even though they contained 68 tons of MIC. The

result was the worst industrial disaster in history, which killed 16,000 to 30,000 people and seriously injured well over 500,000 others, when an uncontrolled reaction occurred in one of the three MIC holding tanks[ii].

The fact was Union Carbine management had not considered the lifecycle of the plant, and in so doing allowed a design with the capacity to bring suffering and destruction on an unprecedented scale. This is not a risk managed by any SIL level: it is gross incompetence and greed - there is simply no justification ever for any commercial organisation to risk an entire city just to make a profit. The Union Carbide business was subsequently bought by Aventis, who avoid responsibility for the business they bought: they bought the gains without any of the costs. That plant did not require SIL 4 systems: it required shutting down and should not have been given an operating certificate. The SIL 4 level is not intended to cover that level of risk.

10.1.3. Pragmatic means to reducing the risk exposure

It is noted that the methodical approach described in Section 2, and applied to the rebreather in Section 3 of this report, has resulted in the same SIL assignment as if the equipment were to have the potential to kill as many people in a single accident. This is an anomaly that is appropriate for a life critical system that is expected to be produced in the thousands, and some variants of that product used by the general public.

Overall, from a pragmatic viewpoint, the SIL 4 assignment for the rebreather that resulting from the application of the formal method for SIL assignment in Section 3, seems sound. It is accepted that other companies may take a different view for a single rebreather produced in very low volume and used only by highly trained commercial divers: in that case a SIL 3 assignment would be justified from the initial assessment onwards.

A means to reduce the SIL 4 assignment to a SIL 3 is to ensure the equipment can be recalled, such as putting in a countdown timer to annual service, then disabling the equipment if the service is not carried out. This would reduce the risk that one design mistake can cause multiple fatal accidents. All Open Revolution rebreathers use this means for risk containment, so from a pragmatic risk perspective should be assigned SIL 3.

10.1.4. Controllability Approach

The controllability approach is also qualitative and consequence based but gives qualitative terms for the acceptable failure frequency associated with each SIL (see Table 2). Each safety function is classified according to the controllability of the motor vehicle should the safety function fail.

Table 1: SILs assignment to controllability categories according to MISRA[iii]

Controllability Category	*Acceptable Failure Rate*	*Integrity Level*
Uncontrollable	Extremely improbable	4
Difficult to control	Very remote	3
Debilitating	Remote	2
Distracting	Unlikely	1
Nuisance only	Reasonably possible	0

For the equipment under consideration the failure of the control system, or to monitor CO2, would likely cause the equipment to be difficult to control or in extreme cases, uncontrollable.

If the diver is able to bail out, the situation may be difficult to control. That is, bail out has to be provided to limit the controllability category of the equipment to avoid it becoming uncontrollable.

If the top side monitoring system fails, the failure would be distracting, but would not be debilitating.

These assessments using the controllability approach, reinforces the SIL assessment through the formal method in the previous section of this study.

10.2. Ethical Acceptability of Risks

A SIL rating is applied to equipment to reduce a risk probability to a level which is acceptable. The HSE Report 216 contains in its Figure 3 a chart listing what is and what is not acceptable: the figure is shown below.

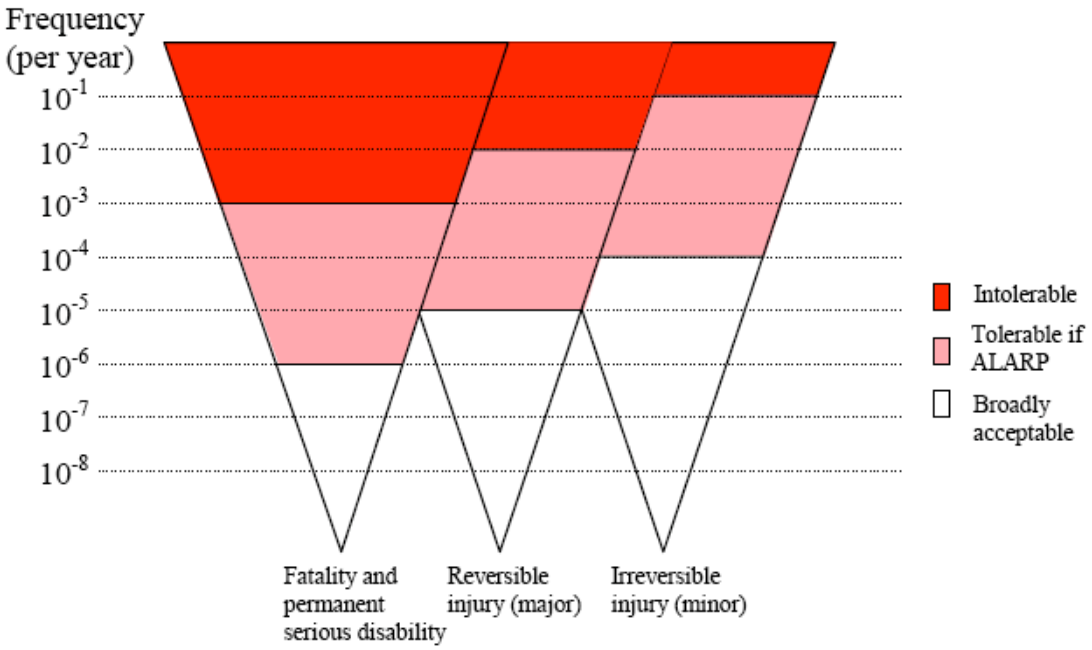

Figure 1: HSE Report 216, Fig 3, charting acceptability levels in risk assessment.

The result of a rebreather developing a fault in the PPO2 control system, or a CO2 fault, or even a WOB fault, is generally a fatality. The equipment is used for hundreds of hours a year when used by professional instructors, and can be thousands of hours a year when used in rotation by commercial divers. In this case the reduction in risk to move the rebreather operation from the frequency without the safety systems, to the “broadly acceptable” level indicated by the UK HSE, is 10^9: again SIL 4.

Debate of this topic with a SIL 3 to SIL 4 audit team, concluded that the use of SIL 4 rigour for a SIL 3 system design was appropriate, but the resulting system would be SIL 3 from the HSE Report 216 Fig 3 because diving is an activity with inherent risks, which become tolerable by the application of ALARP. This process puts the rebreather controllers into the bottom part of the “Tolerable if ALARP” category in the above graph: the border between tolerable and broadly acceptable.

The limiting factor in rebreather SIL attainment, is the limit of diversity in the oxygen sensing.

The complete failure of the top side system is too difficult to assess using the plausibility and risk acceptability method captured in the above image. The Open Revolution project provides a safety barrier in the form of safe rebreather control on the diver.

10.3. UK HSE Diving Risk Data

The UK Health and Safety Executive published a report "Offshore Technology Report – OTO 97 805, Diving Data Manual", December 1997[iv] for the offshore industry giving tables of risks for commercial diving, based on reported safety incidents. The report uses the Markov approach where a fault probability is applied to nodes of a fault tree.

Whilst a full fault tree exists for the equipment under consideration (FMECA Vol. 7), the risks listed in the HSE report are difficult to correlate with sports diving, where the observed incidence of the accidents listed is very significantly higher than that quoted for the highly trained commercial divers. The data relates to surface supplied diving to 50msw only.

11. CONCLUSION

The following Safety Integrity Levels are assigned:

1. The eSCR, eCCR and mCCR is a SIL 3 system that should be designed with SIL 4 rigour, which reduces the risk-cost from a range of 64 to 128, down to a range of 4 to 8. This result is the societal risk that divers assume.
2. The MUX and Topside Unit is a SIL 2 system which reduces the risk-cost from 16 to 2.
3. The Topside Software is a SIL 1 system which reduces the risk-cost from 8 to 1.
4. The independent PPCO2, PPO2 and PFD monitor is triple set of SIL 2 systems, each which reduces the risk-cost from 16 to 2, that operate together to achieve SIL 3.

---

[i] M. Charlwood, S Turner and N. Worsell, UK Health and Safety Executive Research Report 216, "A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines", 2004. ISBN 0 7176 2832 9

[ii] Dominique Lapierre and Javier Moro, "Five Past Midnight, The Epic story of the world's deadliest industrial disaster". ISBN 0-446-53088-3. Half of the proceeds from sales of this book go towards helping victims of the Bhopal disaster.

[iii] MISRA, " Development guidelines for vehicle based software" 1994, ISBN 0952415607

[iv] HSE "Offshore Technology Report – OTO 97 805, Diving Data Manual", December 1997[iv], available from HSE Information Services, Information Centre, Broad Lane, Sheffield S3 7HQ. Tel: 0541 545500.