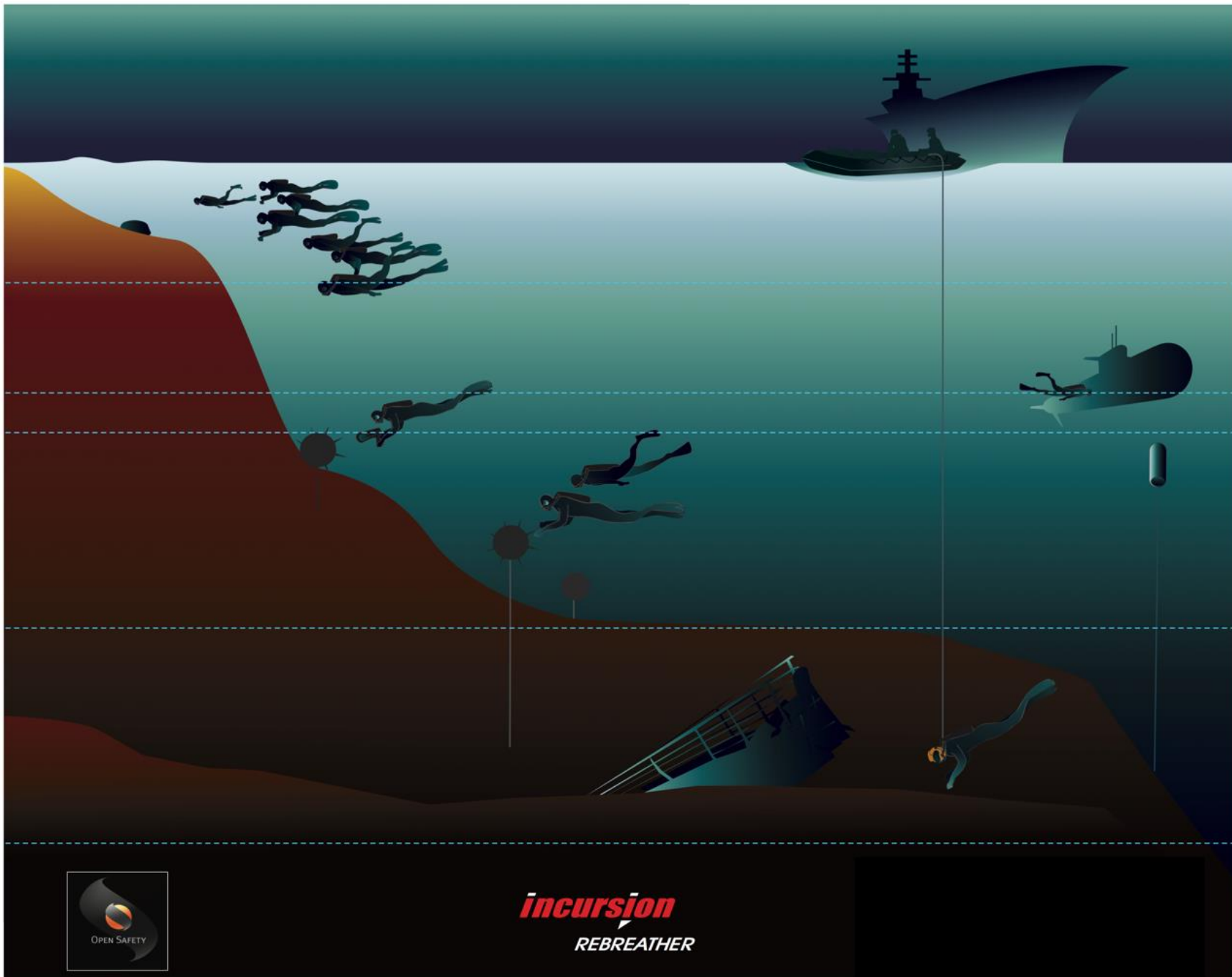




Application of Functional Safety to Military Diving



0 to 8m in CCR mode
on 100% O₂

to 18m in SCR Mode
on 60% O₂
to 24m in SCR Mode
on 50% O₂

to 30m in SCR Mode
on 40% O₂
30m

to 40m in SCR mode
on 32% O₂

to 60m in SCR mode
on Trimix 23

to 100m in SCR mode
on Heliox 16

to 200m in SCR mode
on Heliox 8



Incursion
REBREATHER



Credentials

Open Safety are the only company in the whole of the dive industry to have been certified to a recognised functional safety standard. We specialise in respiratory systems: rebreathers, full face masks, gas protection.

Open Safety have been shipping rebreathers in volume worldwide since 2009, with zero safety mishaps.

Open Safety have four models of rebreather CE certified, and two other models have corresponding national certifications outside the EU, in volume production.

Open Safety work with Apollo Military, Northern Diver, and other Tier 1 suppliers who provide a “one-stop shop” covering everything needed for tactical diving.

Your speaker: 44 years in safety engineering, from science apprenticeship at Harwell Laboratory (Europe's foremost nuclear laboratory), through to PhD, led the microelectronics section at Harwell, Fellow of the Institute of Engineering and Technology. Lead in Functional Safety. Diving since 1979, expedition diver (100m+ certified on SCUBA), dive tech, O2 tech. CEO of Open Safety.

Key Aspects of Functional Safety

1. Understanding hazards: HAZOPs, Accident Studies, FMECA
2. Requirement for Formal Modeling
3. Formal Proof that Equipment is Correct and does not have unknown failure modes
4. Whole lifecycle management
5. ALARP: Risk mitigated to be As Low As Reasonably Possible
6. Independent Assessment

Functional Safety Benefits

1. Lifetime warranties
2. Lifetime safety or performance upgrades, without charge
3. No surprises: it is surprising how many there are in dive equipment
4. Open disclosure

i.e. all things users want but suppliers resist doing

At the higher Functional Safety levels, there is no option except to deliver these.

Why? Answer: ALARP

Reduce the risk to As Low As Reasonably Practicable

Lifecycle from concept to final disposal → responsibility does not finish with shipment

End to End: includes operator & connection to ancillary equipment

If a part has a manufacturing defect, it cannot remain in use → lifetime warranty

If the manufacturer is aware of a means to improve the safety, then it must be provided → lifetime safety upgrades without charge

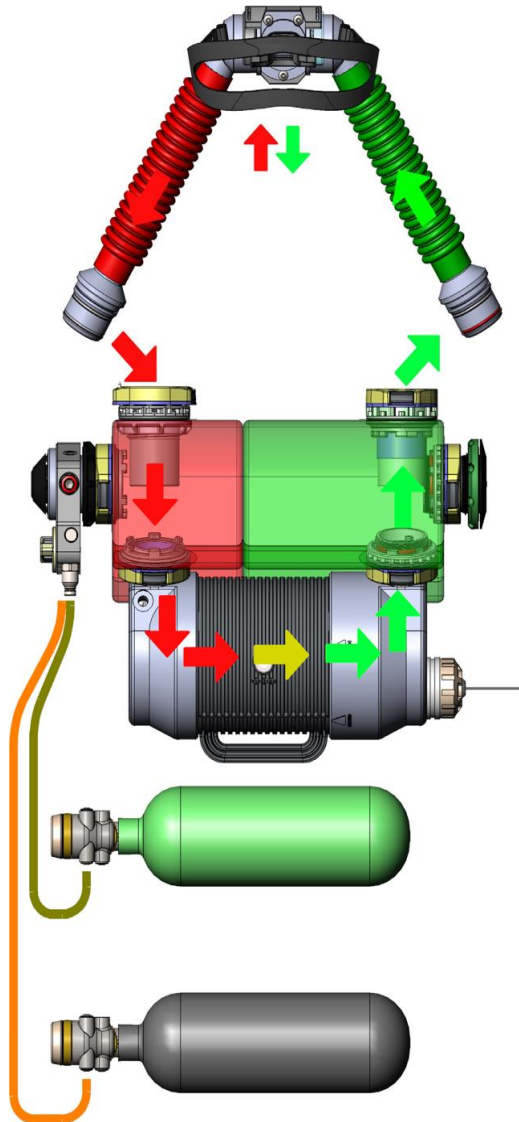
A charge is an impediment to adoption of a safety improvement → not acceptable

Safety Integrity Levels

SIL Level	PDF per hour	Applied where risk of	Examples
0	Any number	No injury or fatality	Table
1	1 in a million	Injury	Medical shower
2	1 in 10 million	Fatalities < 20	Aircraft
3	1 in 100 million	More than 20 fatalities	Mass produced RBs
4	1 in a billion	Mass fatalities	Nuclear Reactors

PDF: Probability of Dangerous Failure

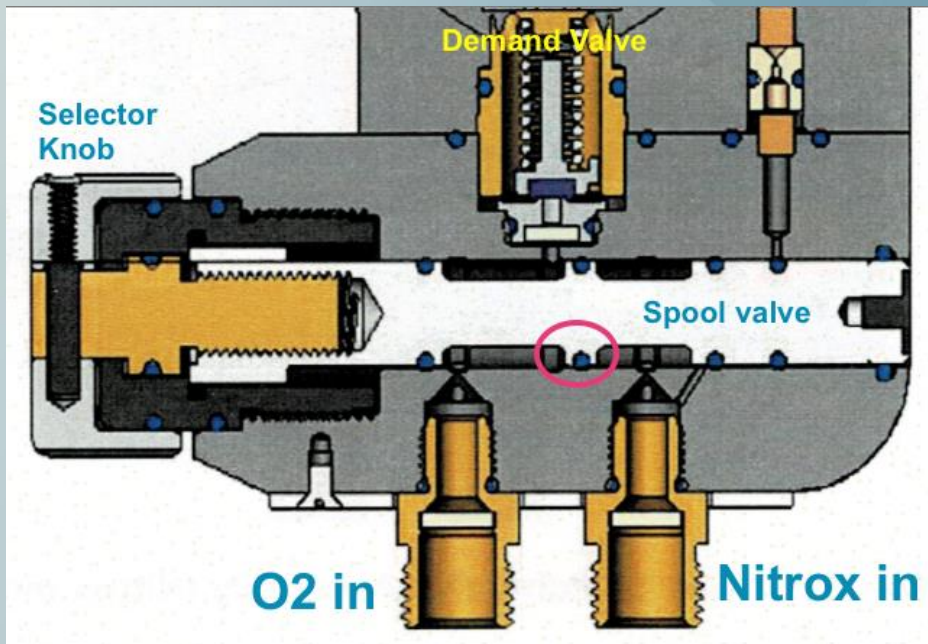
This table is for equipment that has to operate to provide safety, e.g. rebreathers.
Alarms and monitors that activate only rarely are allowed 10,000 times more failures for the same SIL



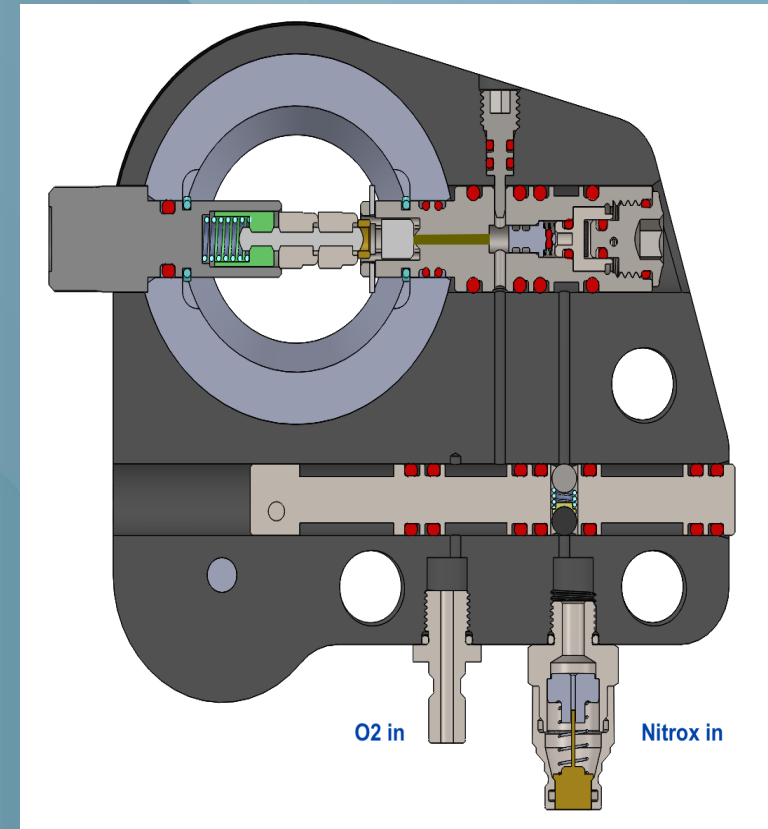
Example: O₂-SCR Switches

In O₂ mode, if Nitrox leaks in, result is hypoxia

Non-FS vs FS: gas switches



Rebreather O2 – SCR switch in use in European Navies,
one o-ring from disaster (no redundancy)



Rebreather O2 – SCR switch in use in Asian Navies,
triple redundancy (quad redundant in use)
dual technology

Other Rebreather Examples

Risk	Typical Performance	SIL 3 Performance
Flood	Caustic cocktail	Fully flood recoverable. Diveable flooded.
Hypercapnia → O2 seizure	2.2 J/L to 5J/L WOB Real deadspace up to 1L	1.4J/L WOB Real deadspace <0.2L
Mission risk	Prebreathe, slowly	Instant on, max RMV
Weight ready to dive	Up to 34kg	<6kg, <11kg, <18kg
Field Maintenance	Tools	No tools
Materials	POM (Delrin), Rubbers	ASA, TPU: non offgasing, safe, strong
PPO2 readings	Some rec RBs have many fatalities from water block, hanging etc	Free of serious defect, zero mishaps in any market sector

Lithium Batteries

ATEX & IEC Ex batteries, 33% lower capacity for same size

For Functional Safety, all failure modes must be assessed

- Floodable.
- Crushable without temperature overrun or flame.
- Pierce without temperature overrun or flame.



Achieved using both LiFePo and LiMn chemistries, BUT at the cost of capacity

33% lower capacity, means:

- 50% increase in performance per watt required for device, or
- 50% bigger battery

Important in diver propulsion, navigation, rebreathers

Specifying FS in contracting

1. Insisting on audited IEC EN 61508 for all electronics & software
2. Insist on EN 61508 or equivalent for mechanics using end to end scope as basis
3. Be aware, response of dive industry was to remove FS from EN 14143 in 2013 revision
4. Specify lifetime warranty
5. Specify lifetime safety upgrades: it can be done

Specifying FS in contracting

1. Insisting on audited IEC EN 61508 SIL 2 or SIL 3 for all electronics & software
2. Insist on EN 61508 or equivalent for mechanics using end to end scope as basis
3. Be aware, response of dive industry was to remove FS from EN 14143 in 2013 revision
4. Specify lifetime warranty: if it is a Functional Safe system, then it is your right
5. Specify lifetime safety upgrades: it can be done

Summary

Functional Safety can:

1. Eliminate hidden equipment risks
2. Keep equipment up to date with best available performance and technology
3. Provide lifetime warranties
4. Improve performance of equipment as supplier wishes to avoid risk from above

It is easily specified in dive equipment contracts and suppliers CAN rise to that goal.