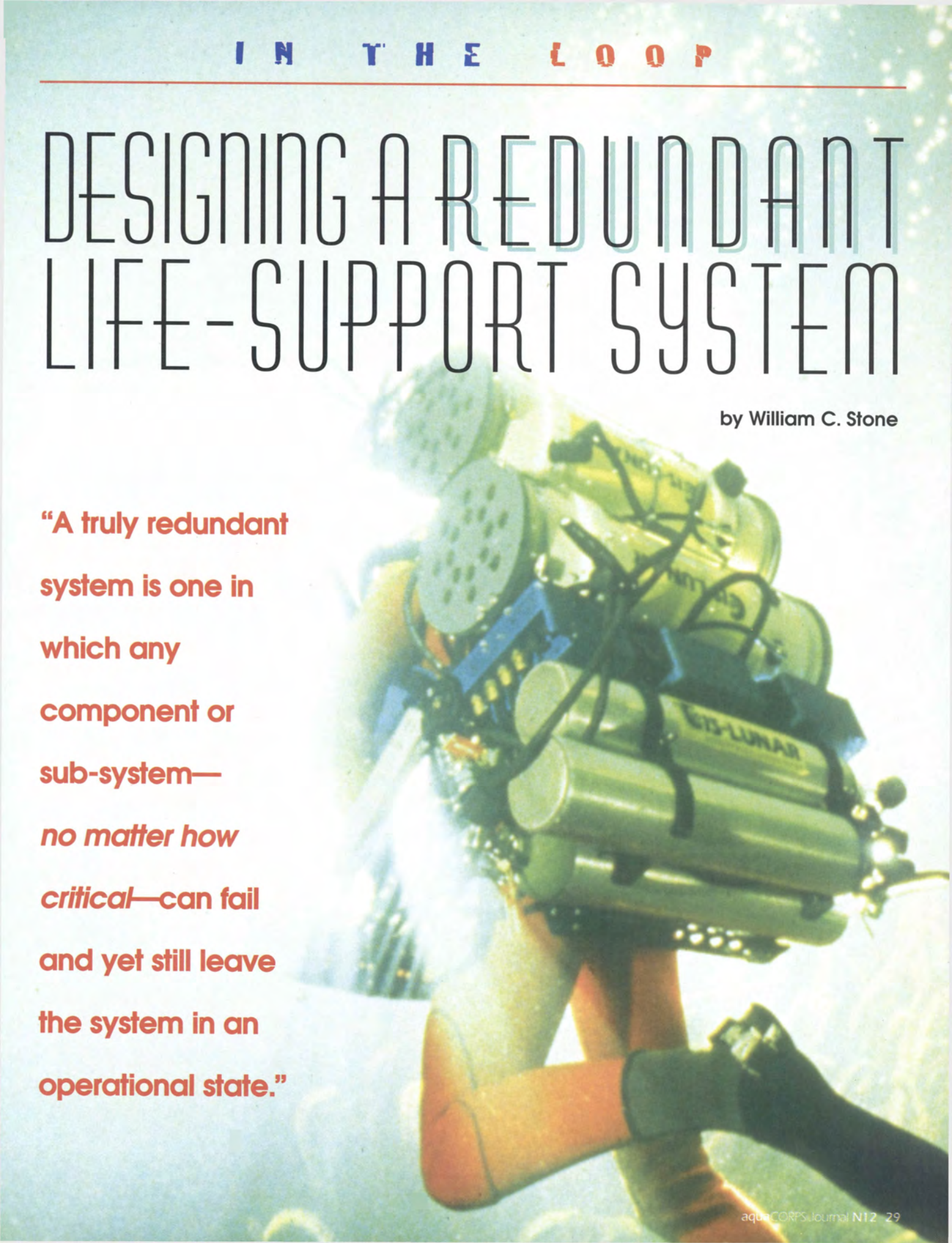
DESIGNING A REDUNDANT LIFE-SUPPORT SYSTEM

by William C. Stone

"A truly redundant system is one in which any component or sub-system—*no matter how critical*—can fail and yet still leave the system in an operational state."



Redundancy has long been the watchword in technical diving circles. For good reason. Murphy loves divers of all kinds, particularly tekkies, and the ability to recover from an equipment failure underwater is generally paramount to survival. No one knows this better than underground explorer and rebreather designer Dr. Bill Stone.

A mechanical engineer by training, Stone designed his first fully-redundant rebreather, the Cis-Lunar MK1, in 1987 as part of the milestone Wakulla Springs Project. Now, five generations and thousands of underwater hours later, Stone's Cis-Lunar Development Labs is preparing to introduce the fully-redundant MK5 system—an upgrade from the system that Stone's team used to explore the Huautla Plateau in Central Mexico [see "Stoned," N7/C2]—that will be used for the Wakulla 2 project [see p 62].

Here in his classic 1989 treatise on life-support systems, Stone explains some of the basic concepts, methodology, and philosophy behind the design of redundant systems that has guided the development of Cis-Lunar's rebreathers.

Survival Probability

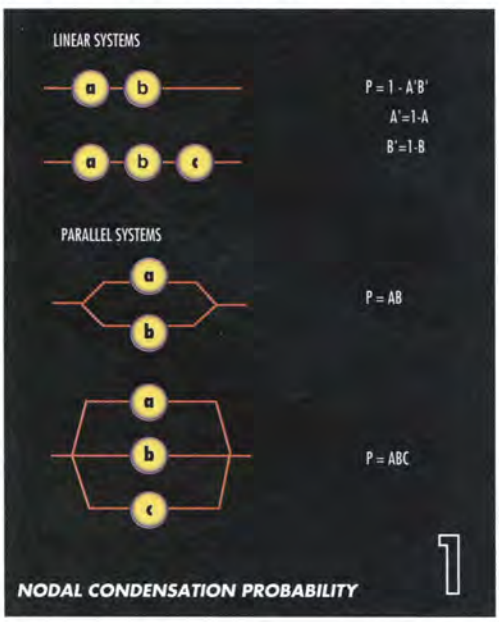
The chief means of achieving true dependability and safety in life-support equipment is by building redundancy into the system. Redundancy implies that several critical components in a life-support system can fail and still leave the user with a functional system.

Just what do we mean by redundancy, and where is it needed? To begin, we need to define a few terms.

The first is *System Failure*. By this we mean that the portable life-support system has ceased to function and will result in the death of the user unless he or she is able to effect an immediate abort to a safe haven. A safe haven could be taken, for example, to be the water's surface, a diving habitat, or a submarine. In the design of life-support apparatus used in critical locations (such as cave diving), we would like to keep the probability of a system failure to an extremely low value.

In general, the more remote we are from the safe haven, the more unacceptable the prospect for a system failure. In fact, we would like to be able to tolerate a few parts failing and still be able to go on with our job, since in such locations one has likely invested considerable sums of money, time, and effort to train a specialized person or team and place them in the field.

This brings rise to the term *Mission Failure*. Here we refer to the state of affairs where the system is still operational, but some parts of sub-systems have failed in such a manner as to limit the range of the device. In other words, the mission has to be scrubbed because the individual cannot reach his objective or finish his task because the duration of his life-support device has been shortened. While mission failures are certainly not as serious as system failures, it is desirable that they too have a low probability of occurrence.



COMPONENT RELATIVE FAILURE PROBABILITY

The percentage listed for each component is an absolute failure probability. In normal fault-tree analyses, these numbers are assigned a lifetime as well, such that we might have a 1% probability of failure in ten years. These can then be used to evaluate the "mean time between failure" statistic that is the general measure of reliability in the aerospace industry. For this simplified life-support reliability study, I assigned these probabilities to the overall lifetime of the rig, which most would assume at around five years (the depreciation rate for high-tech gear).

t	tank (o-ring seal)	1.0%
ie	isolation element	0.1%
i	instrument (gauge, etc.)	1.0%
j	hard-lined junction	0.5%
v	manual valve	1.5%
vm	manual bypass valve	1.5%
vs	servo valve	3.0%
va	auto add valve	1.5%
sc	scrubber stack	1.0%
h	flex breathing hose	1.0%
m	mouthpiece (regulator)	1.0%
fs	first stage regulator	2.0%
s	second stage regulator	2.0%

We can now define redundancy in terms of the failure modes just described. A redundant system is simply one in which a mission failure is possible. To state that more precisely, a truly redundant system is one in which any component or sub-system, no matter how critical, can fail and yet still leave the system in an operational state. Furthermore, it will be shown that by certain arrangements of components, it is also possible to minimize the probability of a mission failure for any given system.

A detailed fault tree analysis involves establishing probability distributions for each component —not so easy in reality—and using this data to derive confidence intervals on a likely outcome.

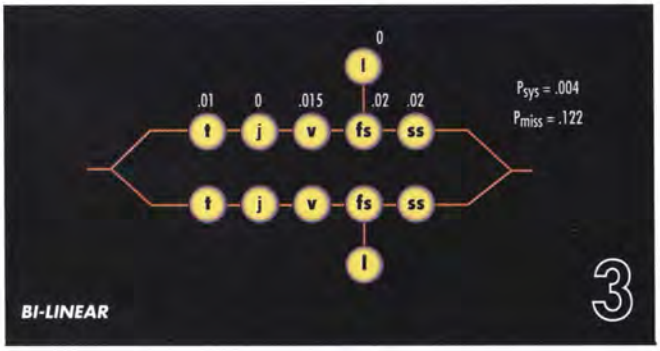
System Failure Probability Analysis

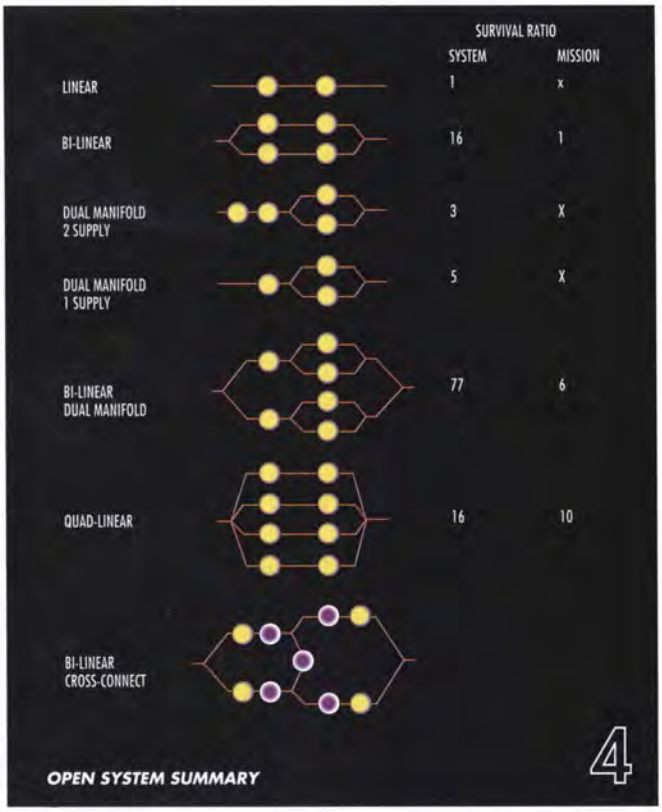
In order to examine the characteristics of life-support systems, a few probability laws need to be introduced. In this discussion, it is assumed that a life-support apparatus consists of a network of interconnected components whose individual probabilities of failure are independent and otherwise unaffected by the failure of any other component in the system. A sub-system consisting of a string of linearly-connected components has a probability of failure equal to one minus the product of the complement failure probabilities—in other words, the probability of success—for each part in that sub-system. A parallel system of components has a joint probability of failure equal to the product of the individual failure probabilities (see Figure 1). These techniques can be used to condense complex systems to a series of equivalent nodes, which can then be reduced to a system failure probability.

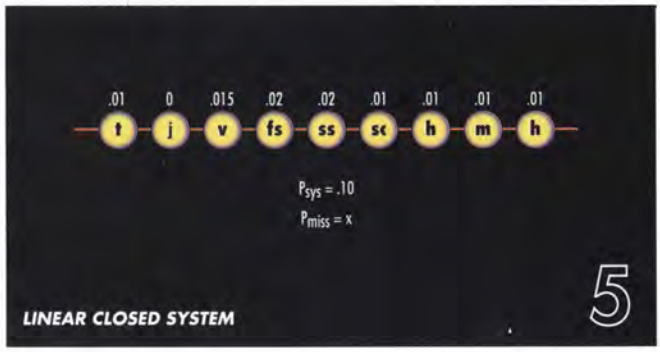
For the sake of comparison with other systems, it is necessary to define failure probabilities for certain types of system components. These can be assigned proportional to their degree of complexity and integration. For example, it may be assumed that a 20,000 psi-rated stainless Swagelok tube junction will, for all practical purposes, have a component failure probability of approximately zero when the gas pressure it normally carries is limited to 150 psi. On the other hand, certain components such as tank o-rings, for example, have been known to blow, although the likelihood of that occurring is small. As the complexity increases, one can, for example, assign a higher probability of failure to a first or second stage regulator. A servo valve, typically used in closed systems, is assigned a still higher probability, since it involves both mechanical moving parts and an electronics interface which can also fail. Although these values are arbitrary, they will serve as suitable relative probabilities for comparing different systems. The table on page 30 gives the probability values used for the evaluation.

Open-Circuit System Analysis

The principals of redundant design can be best illustrated with a few examples in which familiar open-circuit systems are analyzed. Figure 2 shows a probability schematic for the simple one-tank, one-regulator situation, described above as "unsafe" for cave diving. The schematic shown in Figure 2 consists of a linear network of components. The resultant system failure probability is simply one minus the product of the complement failure probabilities for all components. The shape of the network, i.e., a straight line, gives an effective visual picture of its safety shortcomings: a break at any point will cause the device to cease to carry out its function of delivering air to the diver. This is known as a linear system.





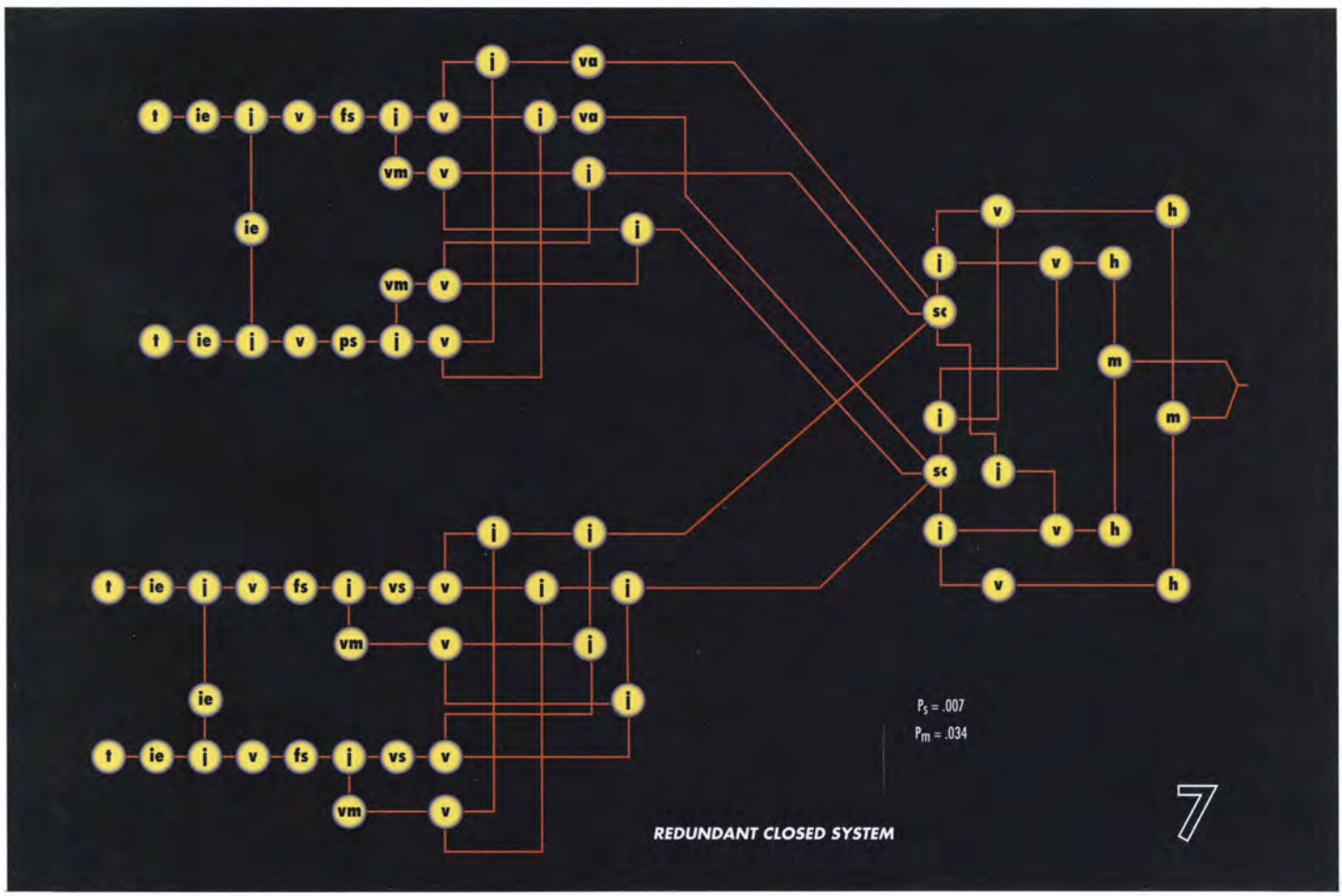


The fundamental attribute of a linear system is that failure in any part of the apparatus causes a system failure. The redundancy level for this system is thus equal to zero. There are several methods for increasing the survival during a cave dive when this type of system is used. One method would be to simply employ two separate independent systems. This "bi-linear" system (Figure 3) is simply the British cave diver's "sidemount" rig (or the "Twin K" or independent cylinders system used by some US wreck and sump divers). The probability of a system failure is theoretically sixteen times less than for the linear system, and it can tolerate a sub-system failure. For later reference, we will define the level of redundancy for this system to be equal to one. The drawback to this rig is that it is complex to use.

In order to understand this last statement, it is necessary to digress for a moment to consider the subject of consumables management. Theoretically, if a tank had an hour's worth of air in it, one could travel from a safe haven to a point a half hour away, and safely return. In practice, however, this does not work. Any delay on the return trip would result in death. So, how much margin do you give yourself? The rule which has become universally accepted by cave divers is to use no more than one-third of the initial starting supply for exploratory work [see "Blueprint For Survival 2.0," p 37]. The remaining two-thirds is reserved for exit. The rationale is that if a partner's life-support apparatus suffers a system failure at the point of maximum distance from the safe haven, there must be sufficient reserves to get both divers out.

Employing a gas consumption rule with a bi-linear system is difficult, since one cannot breathe out of both tanks simultaneously. To really achieve a system failure probability decrease of sixteen, one must first breathe one-third from one tank, switch regulators, and breathe one-third down from the other, and then promptly return, usually effecting another switch on the way out. If this procedure is not used, one runs the risk of breathing down the supply in one tank, only to find a problem with the remaining tank. On the other hand, a regulator switch is never a simple maneuver on a cave dive. At any moment a number of stress risers may also be present: an entanglement with a safety guideline or a load of equipment; zero visibility from either silting or a total lighting system failure; and narcosis effects, to name a few.

For this reason, a great deal of thought has gone into the design of redundant systems where both output sub-systems can access the entire gas supply. Several such designs are summarized in Figure 4. The "Dual Manifold, 2 Supply" system is the Benjamin "Dual Valve Manifold," still in common use by Florida cave divers. However, from a system failure standpoint, it is not as good as a bi-linear system, since any failure in the hard-lined supply will drop the entire system. This is not as unlikely as it may sound: several cases have been reported in which such a failure was triggered by impact with the ceiling while riding a DPV. Thus, what would at first appear to



be a redundant system is, in fact, a modified linear system.

In the early 1980s, Sherwood Selpac introduced a variation of the dual-valve manifold, known as the "Y" valve (see "Dual Manifold, 1 Supply" in Figure 4). This also permitted the attachment of two output regulators, but eliminated several o-rings and hard joint connections by means of a monolithically-cast housing. While this is an improvement over the dual-valve manifold in terms of safety, it is nonetheless still a linear system. In addition, it can only be connected to a single tank, and thus the system is usually range-limited. The best open-circuit architecture yet devised, from the viewpoint of both system and mission failure, is the "Bi-Linear Cross-Connect" system (Fig-ure 4). This is a bi-linear system with a flexible high-pressure manifold and a series of isolation elements. Provided that the isolation elements have a low probability of failure (e.g., an extremely reliable shut-off valve), this system combines the best features of dual manifold design and bi-linear supply. The resulting system is ten times less likely to suffer a mission failure than a simple bi-linear system. It is, in fact, the first truly redundant system that has been discussed, in that any system output component can access any gas supply. Further, any faulty component can be isolated from the system in the event of a failure.

Closed-Circuit System Failure Probability

Figure 5 shows a probability schematic for a simple oxygen rebreather. From the principles just discussed, it is immediately apparent that this is a linear system, since failure of any part will cause failure of the system. Likewise, because there are more components in the system, the probability of failure is higher than for a simple linear open system. The probability schematic for a typical mixed-gas rebreather is shown in Figure 6. Once again, this is a fundamentally linear system, with the exception of the parallel sub-systems which bypass the second stage diluent regulator and oxygen solenoid valve. These bypass valves are a definite step in the right direction, but because failure in any sub-system—that is to say either of the two supplies, or the processor—can cause a system failure, this is not a redundant system. As such, it cannot be considered safe for cave diving missions.

Fully-Redundant Rebreathers

To begin a discussion of fully-redundant closed-circuit scuba, the lessons learned from the design of open-circuit systems may be recalled. The first factor to consider is that true redundancy is only achieved when there are multiple output paths which can independently access any of at least two independent supply systems. Addi-tionally, all sub-systems must be capable of being isolated from the overall system in the event of their failure. This can be achieved on a sub-system basis by using the previously developed "Bi-Linear Cross-

A BIT OF REDUNDANCY

1 System failure probability can be decreased by providing multiple, independent life-support systems (consisting of a gas supply and access and control path to the user) within the context of a single-user device. Increasing the number of paths (gas supplies and output lines) decreases system failure probability in proportion to the product of the individual path failure probabilities. However, system management becomes overly complex when more than two independent output paths are employed.

2 Mission failure probability can be minimized by providing full cross-connections between the gas supplies and output paths. Each cross-connect node must be capable of being isolated from the system in the event of a component failure.

3 The simplest fully-redundant life-support architecture is the Bi-linear Cross-connect, in which two gas supplies drive dual, independent output lines, which are joined by means of a high pressure cross-connect line. Each end of the cross-connect line contains a three-way junction in which each output path from the junction can be closed.

Connect" architecture. For a Type I diluent (e.g., Heliox or Trimix) supply, this is shown as in Figure 7. Here a bi-linear cross-connected open system has been integrated with two independent processor circuits. Note that the second-stage manual bypass circuit has been retained in order to reduce the probability of a system failure should a failure occur in the second stage. Furthermore, note that there are two independent delivery lines to each of the two processors. A similar design can be used to construct a Type II oxygen supply for this system. The principle difference between Type II and Type I supplies, again, is that the second stage regulators used in the Type I supply have been replaced with servovalves.

The next step involves the construction of a parallel processor output system (right half, Figure 7). Unfortunately, in closed-circuit diving operations one cannot make use of a cross-connect system, since a leak in the active output line would subsequently flood both scrubbers. Therefore, to safely achieve mission range, the user must switch processors during the dive and make use of the "thirds" consumption rule (in this case applied to scrubber duration). However, turning a directional valve is substantially less stressful than having to switch mouthpieces, as would be the case with a bi-linear system.

For serious cave diving, where an open-circuit abort scenario is not possible, full closed-circuit redundancy is mandatory.

The system survival probability for the redundant rebreather is approximately fourteen times greater than that for existing mixed-gas rebreathers. Moreover, the mission success rate represents a four-fold increase over that for a simple bi-linear open-circuit (British sidemount) architecture, and that is a strong statement when one considers that the mixed gas system is substantially more complex. There is no comparison with existing Naval rebreathers on a mission failure basis, since none are redundant.

The fully-redundant architecture described above was implemented by Cis-Lunar Development Laboratories, Inc. in its MK1 experimental rebreather which was tested at Wakulla Springs during the project.

Bill Stone is Chairman of Cis-Lunar Development Laboratories, Inc. He holds seven patents and has been responsible for the design of five generations of fully-closed-circuit life-support backpacks, including the MK5 system which will make its debut at 96 tek. He has organized 27 expeditions related to cave exploration and was the leader of the 1987 Wakulla Springs Project. In 1994, he used the Cis-Lunar MK4 system to crack Mexico's San Agustin Sump, at a depth of 4,347 f/1,325 m beneath the surface. This article is excerpted from The Wakulla Springs Project*, edited by William Stone (US Deep Caving Team).*