Design of Extended Range EVA PLSS Systems: Lessons from Terrestrial Exploration Missions

William C. Stone
National Institute of Standards and Technology
Gaithersburg, MD

ABSTRACT

As plans progress for construction and maintenance of the international space station and, more importantly, private missions to LEO and beyond become viable, serious thought will need to be given to re-engineering EVA (space suit) systems to achieve greater range and reliability at dramatically reduced cost. This paper discusses alternative architectures for fully closed cycle portable life support systems (PLSS) that have been built and tested over the last decade for use in hazardous subaquatic environments. Fault tolerant design, both for the mechanical and computational hardware elements, was employed in the development of four generations of prototype devices. The culmination of these designs was successfully used to explore a 600 meter long underwater tunnel which began at a depth of 1353 meters vertically beneath the surface of the earth in southern Mexico. Lessons relating to survival and range enhancement on orbital and lunar EVA missions are presented.

Introduction

We stand now on the threshold of a new era in spaceflight, where private entrepreneurs have begun serious efforts to breach the cost barriers that have made space the domain of government robots and a few fortunate government employees. At least six groups have declared themselves contenders for the "X-Prize". Others are more quietly courting venture capital funding to compete for the much larger prize -- the launching of the Teledesic, Iridium, and other personal communications satellite networks. And there is serious talk of space tourism, driven largely by the anticipated reduction in launch costs that will be achieved through economy of scale in deploying those satellites. For the X-prize and space tourism, issues will soon arise regarding life support systems, both for the crew cabin as well as for spacesuits to be used during launch and for on-orbit extra-vechicular activities (EVA). Servicing of orbital communications infrastructure will further drive demand for EVA systems. However the eventual shake out in launch providers takes place, there will be new demands for "industrial" EVA systems to accomplish tasks that will appear bold by present standards. Those private organizations will not pay $25M a suit, either[1].

In light of the above changes it is worth considering how one might achieve significant cost reductions in EVA systems, while at the same time increasing system range and reliability. A useful cost reduction target seems to be around 1/50th to 1/100th the price of present government-issue shuttle spacesuits. Is this a wild vision, or something that can actually be achieved? In the remainder of this paper I will alternate discussion between simple system failure calculations and practical design considerations for building realizable portable life support systems (PLSS) which could form the "heart" of an industrial suit. The hardware described herein has actually been built and used in very hazardous environments. A great deal of it is commercially available or can be configured from commercial components.

It has been known for some time that aquatic environments provide a useful analog to space, both in terms of "neutralization" of gravity effects (through buoyancy equilibration) as well as being an "airless" environment. The exploration of underwater environments, but specifically the rapid expansion in the field of subaquatic speleology (the exploration of submerged caverns) in the last decade, has fueled the development of sophisticated PLSS units whose range and reliability bear directly on the design of new low cost spacesuit PLSS backpacks. For sake of brevity, discussion of PLSS design herein will be limited to apparatus and systems necessary to sustain human respiration only.

To begin the discussion let us examine a familiar PLSS system: an open circuit Scuba rig. This type of system (Fig. 1) was first introduced by Cousteau and employs a compressed gas supply and a demand regulator from which the diver breathes. The exhaust gas is ported overboard with each breath, hence the name "open circuit". From a functional standpoint, little has changed

---

Reprinted from: Proceedings, 12th Conference on Space Manufacturing, May 8-11, 1997, Space Studies Institute, Princeton, NJ.

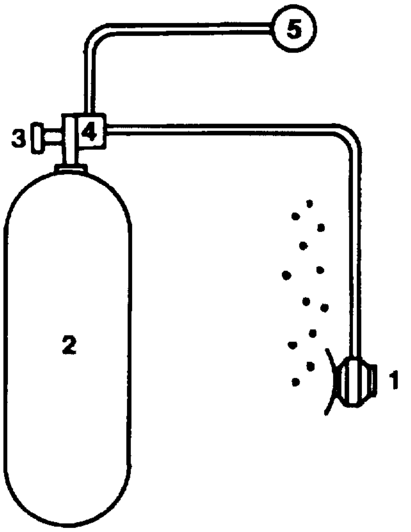

Fig. 1: Traditional Cousteau-Gagnon Open-Circuit Scuba Backpack. 1=Second Stage Regulator; 2=Pressurized Gas Tank; 3=On/Off Valve; 4 = First Stage Regulator; 5= Tank Pressure Gage.

since the 1950's when the single-hose version of this system was introduced. Certain attributes, such as higher operating pressures and lighter tank weights, have been improved through the use of composite technology (now ubiquitous as firefighter SCBA packs), and the first stage regulator yolk, a weak point in original American designs, has been replaced with direct thread DIN connections for use with higher operating pressures. With these improvements the range for open circuit apparatus has, for all practical purposes, been maximized. Beyond 35 Mpa [5000 psi] (the pressure used in composite Scuba) the amount of gas which can be stored for a given increase in pressure becomes smaller because of molecular interaction which follows the real gas laws. Furthermore, at pressures much greater than 41 Mpa [6000 psi], three stage regulators, which are mechanically more complex, become essential. Beyond this, it is possible to use liquified gas supplies but the management of cryogens adds further complexity and is not suited for long term storage in portable systems.

None of these details, however, change the basic characteristic of open circuit apparatus: because only a fraction of the respiratory minute volume (RMV; the volume of gas inhaled and exhaled during normal breathing) is actually used in the sustainance of metabolic function, there is a tremendous waste of useable oxygen with each breath, particularly so if the breathing gas happens to be pure oxygen, as opposed to a mix of oxygen diluted with some other inert gas. In diving apparatus this situation leads to untenable consumables management problems since the quantity of oxygen lost in this manner increases with depth. A mission at 100 m depth underwater involves breathing gas utilization rates which are ten times those at the surface, owing to hydrostatic compression of the inspired gas. A far more efficient PLSS, known as an oxygen rebreather, has been in existence for more than a hundred years. This is the simplest form of a general class of devices known as closed-circuit life support apparatus.

In a closed system nearly 100% use is made of the oxygen content of the supply gas. This is done by recycling the exhaust (diminished in oxygen, but enriched in carbon dioxide) through a scrubbing mechanism -- often an alkaline hydroxide or superoxide, but which could be a more sophisticated chemical, thermal, or electrical based system -- which removes the carbon dioxide.

In a rebreather, oxygen is added to the system only in the amount needed to make up that which is lost through metabolism. The difference in performance over an open circuit system is striking: a 2265 liter cylinder used in open circuit mode at a depth of 100 meters will provide approximately 30 breaths before the tank runs dry; the same cylinder, if filled with pure oxygen and used to drive a closed circuit system, could sustain an individual at 100 meters for more than two days.

There are two types of closed systems in use for diving: a pure oxygen version which is limited to a depth of 8 meters (for physiological reasons related to oxygen toxicity -- not a factor for space related work), and a mixed gas version used for underwater work at great depths. The pure oxygen system is the simplest and will form a starting point for discussion of more complex sytems. An oxygen rebreather (Fig. 2) consists of a linear open circuit oxygen delivery system driving a "process" loop, in which the user breathes from a flexible counterlung attached to the carbon dioxide scrubber. The counterlung serves as a compliant volume which accepts the exhaled gas from the user. In a spacesuit, the compliant volume can be accomodated by the interior of the suit itself. Likewise, in the subsequent discussions one should bear in mind that underwater it is the human lung which drives the gas flow in the PLSS, leading to complications which affect the work of breathing. For space suits, the process loop is typically driven by an in-line electrically actuated fan, making for simpler and easier use, but at the expense of additional component complexity.

The exhaust breath in a rebreather is cycled back into the scrubber. As the oxygen is converted into carbon dioxide via metabolism and the carbon dioxide is removed by the scrubber system, the volume of gas in

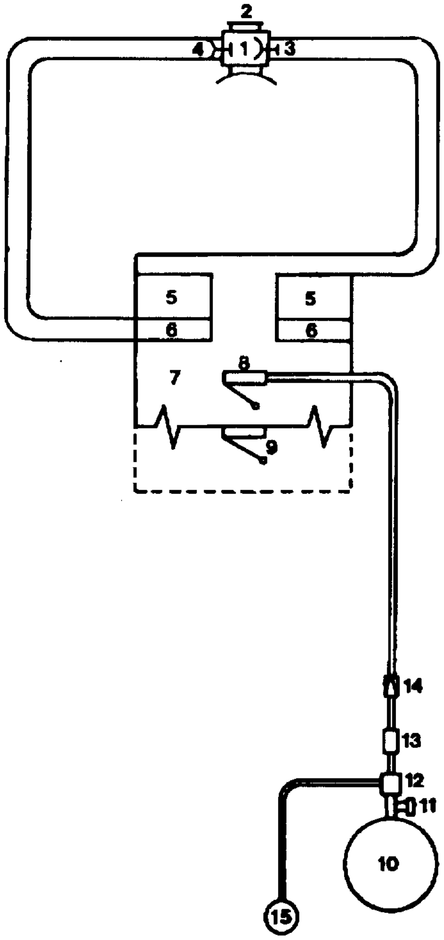

Fig. 2: Oxygen Rebreather Schematic. Components include 1) Breathing Manifold; 2) Breathing Manifold Shutoff; 3) Upstream Checkvalve; 4) Downstream Checkvalve; 5) Carbon Dioxide Scrubber; 6) Moisture Trap; 7) Counterlung; 8) Oxygen Addition Valve; 9) Overpressure Checkvalve; 10) High Pressure Oxygen Supply; 11) Oxygen On/Off Valve; 12) First Stage Regulator; 13) Filter Trap; 14) Metering Orifice; 15) Pressure Gage.

the counterlung begins to decrease. When the counterlung (for diving apparatus) collapses due to oxygen depletion a second stage limit switch is triggered and oxygen is added to the system.

From a control standpoint, oxygen rebreathers are quite simple: they require no active control. This is not the case with mixed gas rebreathers (Fig. 3). These were first pioneered in the late 1960s in an effort to solve the problems of narcosis at depth and to eliminate the oxygen toxicity problems which limit the safe diving depth of pure oxygen rebreathers (again, neither of these physiological complications are at issue for spacesuit PLSS design, but the concept of mixed gas operation is valid where pure oxygen operation is deemed undesirable). A typical sensor controlled mixed gas closed system consists of two independent gas supplies, and a process loop which is regulated by sensors (often electrochemical in nature) which monitor the partial pressure of oxygen [7]. The two gas supplies are functionally different. A "Type I" supply contains a mixed gas "diluent", usually helium-oxygen or helium-nitrogen-oxygen for diving, which could in itself be breathed in an open circuit system within the operating environment of the device. This supply is used to maintain system volume during depth related excursions where the volume of gas in the counterlung and scrubber is compressed. In a spacesuit, this gas would be used solely to establish the initial suit atmosphere and then subsequently only for leak compensation. Depending on the situation there are other

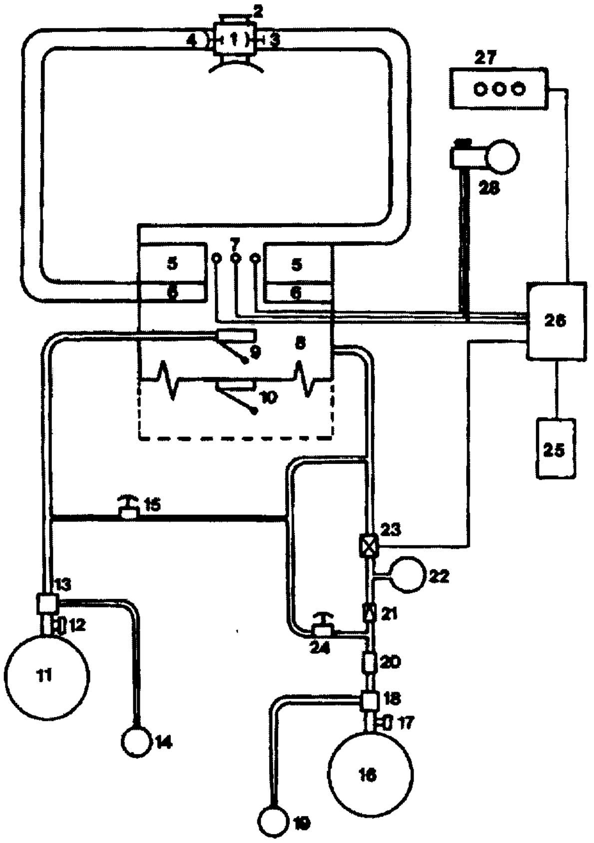

Fig. 3: Mixed Gas Rebreather Schematic. Components include 7) Oxygen Sensors; 11) High Pressure Diluent Supply; 12) Diluent On/Off Valve; 13) Diluent First Stage Regulator; 14) Diluent Pressure Gage; 15) Diluent Bypass Valve; 16) High Pressure Oxygen Supply; 17) Oxygen On/Off Valve; 18) Oxygen First Stage Regulator; 19) Oxygen Pressure Gage; 20) Oxygen Filter; 21) Metering Orifice; 22) Low Pressure Accumulator; 23) Oxygen Solenoid; 24) Oxygen Bypass Valve; 25) DC Power Supply; 26) Logic Circuitry; 27) Primary Display; 28) Analog Display. Parts 1-6 are identical to those in Fig. 2; Parts 8-10 are the same as 7-9 in Fig. 2.

System Failure Probability Analysis

At this point a few simple probability laws need to be introduced in order to examine the characteristics of life support systems. 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. Furthermore, for the sake of comparison, we assume the component failure probabilities to be static. Excellent summaries of static network analysis are given in [2,3,4,5].

A subsystem consisting of a string of linearly connected components (Figure 4a and 4b) has a probability of failure equal to one minus the product of the probability of success for each component in that subsystem. Since the probability of success for a component is given by $P'_a = (1-P_a)$, where P_a is the probability of failure for that component, this can be expressed, for the 3-component system shown in Fig. 4b, as:

$$P_{system} = 1-(1-P_a)(1-P_b)(1-P_c) \qquad \text{Eq. 2}$$

where: P_a is the probability of failure of A

P_b is the probability of failure of B

Pc is the probability of failure of C

From this it is easy to see why one might conclude that the only way to increase reliability would be to reduce the number of components and simultaneouly increase their MTBFs.

A parallel system of components (Figure 4c and 4d), on the other hand, has a joint probability of failure equal to the product of the individual failure probabilities. This can be expressed, for the system shown in Fig. 4d, as:

$$P_{system} = (P_a)(P_b)(P_c) \qquad \text{Eq. 3}$$

These two techniques can be used to condense complex systems to a series of equivalent nodes, which can then be reduced to a system failure probability [2,3]. In a rigorous fault analysis one needs statistical reliability data for each component. For preliminary design, however, we can assign approximate values for failure probabilities for certain component categories. These can be assigned proportional to their degree of complexity and integration and need not be precise. For example it may be assumed that a 138 Mpa (20,000 psi) rated stainless tube fitting will, for all practical purposes, have an extremely low component failure probability when the gas pressure it normally carries is limited to 1 Mpa (145 psi). Gas supply tank o-rings, on the other hand, have been known to blow, although the likelyhood of that occurring is small. Moving up in mechanical complexity one can 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 not precise they will serve as suitable relative probabilities for comparing different systems. Table 1 gives the failure probability rate values used for the evaluation.

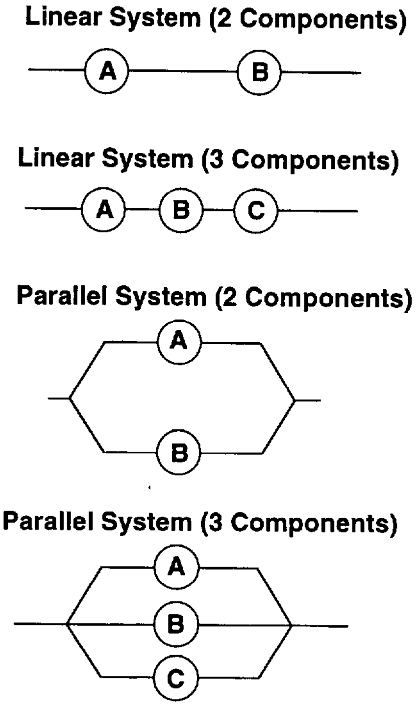

Fig. 4: Typical Mechanical / Electrical Probability Schematics for systems consisting of a) two components in series; b) three components in series; c) two components in parallel; and d) three components in parallel.

Mission Failure Probability Analysis

In redundant system design the intent is to permit a few failures to occur and yet still be able to carry out the mission objectives. How does one quantify "a few failures?" If we consider two parallel PLSS systems, A and B (see Figure 4c), where each system, independently, is <u>just</u> able to provide the necessary life support to successfully complete the mission, we can define, in the limit, the mission failure probability as the probability of losing sufficient components and subsystems so as to reduce the PLSS to its least functional state, short of a

Table 1: Estimated Component Failure and Reliability Probabilities for Typical PLSS Components.

COMPONENT	SYMBOL	COMPONENT FAILURE PROBABILITY	COMPONENT RELIABILITY
Tank (Pressurized Gas)	T	0.01	0.99
Isolation Element	IE	0.001	0.999
Instrument (Pressure Gage	I	0.005	0.995
Hard-Lined Junction	J	0.005	0.995
Manual Valve	V	0.015	0.985
Manual Bypass Valve	VM	0.015	0.985
Servo Valve	VS	0.03	0.97
Auto-Addition Valve	VA	0.015	0.985
CO2 Scrubber	SC	0.01	0.99
Flexible Breathing Hose	H	0.01	0.99
Mouthpiece Block	M	0.01	0.99
First Stage Regulator	FS	0.02	0.98
Second Stage Regulator	S	0.02	0.98
Armored Hose	AH	0.005	0.995
High-Rel 3-Way Valve	HV	0.001	0.999
Dual Seal CO2 Scrubber	DC	0.005	0.995

system failure. In such a situation, one could -- without regard to personal safety -- carry out the mission successfully and still return to base. Since any further component losses would lead to a full system failure, however, practical considerations would dictate an immediate retreat under most circumstances.

The above definition provides a useful means of comparing the level of redundancy in a PLSS. This probability will be referred to subsequently as the **mission failure probability**.

For the case shown in Figure 4c, the mission failure probability is represented by two independent events (the failure of system A or the failure of system B, but not both). The probability that A fails, but not B, is given by:

$$P_a - P_aP_b \qquad \text{Eq. 4}$$

where P_a is the probability of failure of A

P_b is the probability of failure of B

However, the alternative -- B fails, but not A, can also occur and lead to a mission failure. This probability is given by:

$$P_b - P_bP_a \qquad \text{Eq. 5}$$

The mission failure probability for this two-unit, parallel system is thus given by:

$$P_{mission} = P_a + P_b - 2P_aP_b \qquad \text{Eq. 6}$$

This technique can be expanded for three parallel systems to:

$$P_{mission} = P_aP_b + P_bP_c + P_aP_c - 3P_aP_bP_c \qquad \text{Eq. 7}$$

where any two of the three PLSS systems must fail to produce an irreducible, but still operational backpack. It is assumed here that the above events are independent, i.e. that one failure does not trigger another.

When considering what leads to a mission failure one must judiciously search for the least number of things that must fail in order to reach the least operable state. In some cases, just a few sub-systems can have a controlling effect. In order to spot such situations easily it is useful to graphically represent the device by nodal networks.

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. Fig. 5 shows a probability schematic for the simple one-tank, one-regulator design which more than three decades ago was realized to be "unsafe" for cave diving. The schematic shown in Fig. 5 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. System failure probabilities calculated for other architectures below are normalized in Table 2 to this value.

The fundamental attribute of a linear system is that failure in any part of the apparatus causes a system failure. The system has no redundancy, and hence no mission failure probability. There are several methods for increasing survival probability when this type of system is used. One method would be to simply employ two separate independent systems. This "Bi-Linear" system (Fig. 6) is the British cave diver's "sidemount" rig. The probability of a system failure is theoretically 14 times less than for the single Linear system, and it can tolerate a subsystem failure. For later reference, we will define the level of redundancy for this system to be equal to one. One drawback to this rig is that it is complex to use.

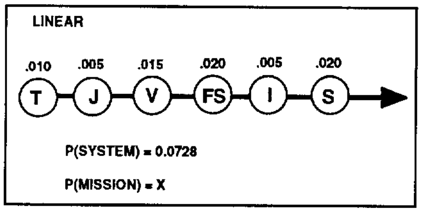

Fig. 5: Probability Schematic for Linear Open-Circuit Scuba.

In order to understand this last statement it is necessary to digress for a moment to the subject of consumables management and human engineering. 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 became universally accepted by cave divers for nearly three decades was to use no more than 1/3 of the initial starting supply for exploratory work. The remaining 2/3 was reserved for exit. The original rationale was that if a partner's life support apparatus suffered a system failure at the point of maximum distance from the safe haven then there had to be sufficient reserves to get both divers out. In practice, this is flawed logic, since two individuals in an elevated state of anxiety will, using open circuit apparatus, consume significantly more gas than when calm, at rest. Thus, many explorers now reduce the amount allocated for outbound transit to 1/4 or 1/5th of the overall supply. For the Wakulla 2 project, set to commence on October 1, 1997, exploration teams will employ multiply redundant, cross linked closed cycle apparatus with 4:1 reserve margins on missions which will reach up to 3 hours duration on the outbound leg (that is, three hours distant from the nearest emergency PLSS depot and approximately nine hours round trip to the safe haven).

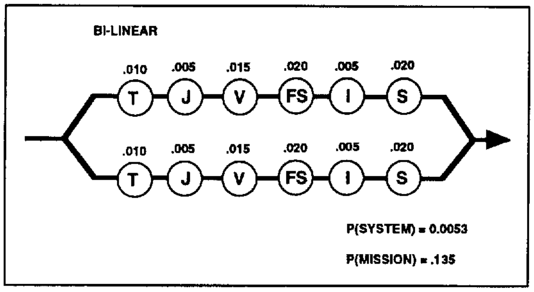

Fig. 6: Probability Schematic for Bi-Linear Open-Circuit Scuba (two completely independent, parallel systems).

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 14, one must first breathe 1/3 from one tank, switch regulators, and breathe 1/3 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. However, 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. Similar lists could be drawn up for EVA work.

For this reason, a great deal of thought has gone into the design of redundant systems where both output subsystems can access the entire gas supply. Several such designs are summarized in Fig. 7. The "Dual Manifold, 2 Supply" system is one which saw common use by technical divers in the 1970s and 80s. From a system failure standpoint, it is not as good as a bi-linear system, since any failure in the hard lined supply connecting the two tanks will cause the entire system to fail. 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 of a flooded cavern while riding an electric propulsion vehicle (the diver's equivalent of an MMU). Thus, what would at first appear to be a redundant system, is in fact a modified linear system. Similar supply systems are used for the present shuttle spacesuit (see Fig. 10).

In the early 1980's a variation of the dual valve manifold, known as the "Y-valve" (see "Dual Manifold, Single Supply in Fig. 7) became available. This also permited 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 (for exactly the reasons expounded in Eq. 1, it is nonetheless still a linear system. Furthermore, 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. 7). 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 a bi-linear supply.

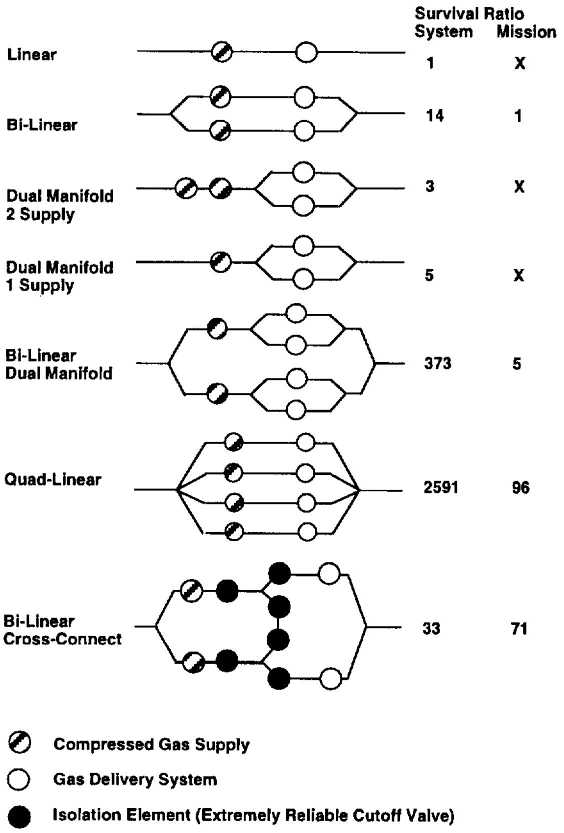

Fig. 7: Probability Schematic Summary for Open-Circuit PLSS Units. The apparent security afforded by four independent output systems (Bi-Linear Dual Manifold) or four completely independent PLSS units (Quad-Linear) is diminished by human factors considerations which prohibit effective management of complex systems. High-Reliability (Hi-Rel) linkages, which cross and separate various subsystems, can significantly increase system and mission reliability, even for simpler systems (Bi-Linear Cross-Connect).

The resulting system is 71 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. Furthermore, any faulty component can be isolated from the system in the event of a failure. Seventy two of these systems, using 3000 liter S-glass composite cylinders, were used to explore 4.2 kilometers into the flooded cavern known as the Pena Colorada in southern Mexico in 1984 [10]. During 640 missions fielded, two mission aborts ocurred. Both were due to accidental closure of valves by contact with the cavern roof, not because of mechanical failure, and were classified as "diver error".

Closed-Circuit System Failure Probability:

Fig. 8 shows a probability schematic for the oxygen rebreather described earlier. From the principles just discussed, it is apparent that this is a linear system, since failure of any part will cause failure of the system. Because there are more components in the system, the probability of failure is higher than for a simple linear open system. A nearly identical architecture is employed in the present shuttle spacesuit, which utilizes a 0.29 bar (4.3 psi) pure oxygen internal suit pressure maintained by mechanical pressure-triggered valves (a second stage regulator). Fig. 10 shows a schematic for the overall shuttle suit PLSS, including both the primary and bailout oxygen supplies. The bailout system provides approximately 25 minutes range, intended to be sufficient to return to the shuttle airlock from any anticipated task in the immediate environs of the shuttle. It is this bailout duration that completely determines the useful range envelope for the spacesuit.

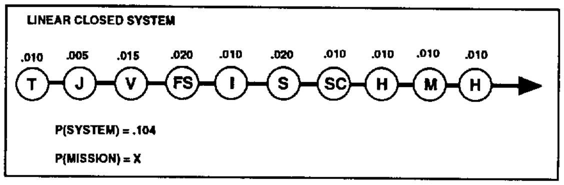

Fig. 8: Probability Schematic for Simple Oxygen Rebreather.

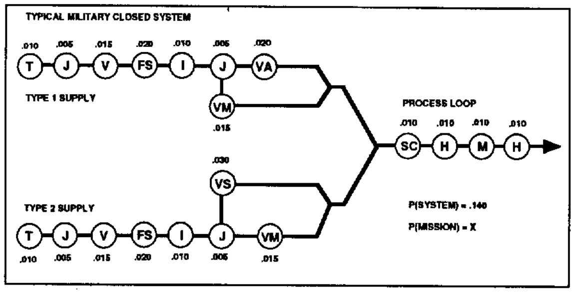

Fig. 9: Probability Schematic for typical Mixed-Gas Rebreather, Commonly Used by U.S. Military Forces.

The probability schematic for a typical mixed-gas rebreather (one using both helium and oxygen gas supplies) is shown in Fig. 9. This is a linear system, with the sole exception of the parallel subsystems which bypass the second stage diluent regulator and oxygen solenoid valve. These bypass valves are, at first appearance, a step in the right direction, but because failure in any subsystem -- that is to say any element in either of the two supplies, or the processor -- can cause a system failure, this is not a redundant system. Furthermore, in the design shown (which is being used by Navy personnel around the world at this time) failure can also occur if

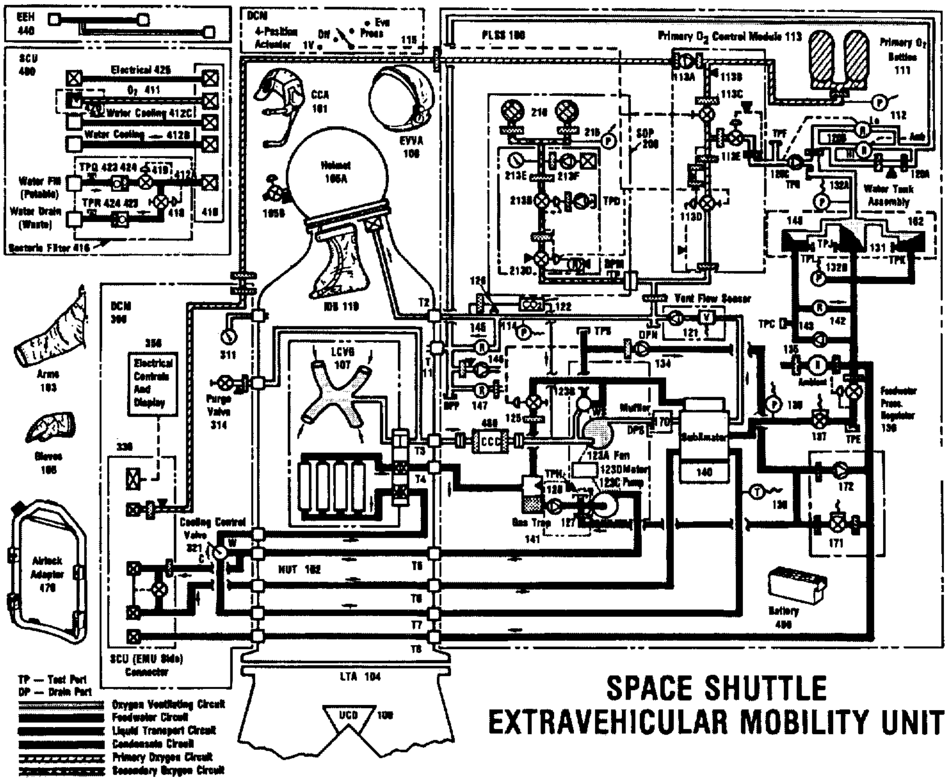

Fig. 10: Functional Diagram for the Space Shuttle EMU. The Primary Oxygen Circuit is shown beginning at the dual-manifold supply system in the upper right. Metabolic gas makeup is accomplished by means of a mechanical constant pressure addition valve. The suit operates at 0.29 bar (4.3 psi) pure oxygen and is a direct implementation of the system class shown in Fig. 8. [courtesy NASA Crew Systems Division, JSC].

either of the bypass or second stage regulators fail in the "redundant" paths, i.e. no means exists in these designs to isolate the flow should one of those valves fail in the open state. Because there are significantly more components than for the case shown in Fig. 8, this system is even more prone to failure.

To begin a discussion of fully redundant closed cycle PLSS, 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. Furthermore, all subsystems must be capable of being isolated from the overall system in the event of their failure. This can be achieved on a subsystem basis by using the previously described Bi-Linear Cross-Connect architecture. For a Type I diluent supply, this is as shown in the upper left segment of Fig. 11. Here a bi-linear cross-connected open system has been integrated with two independent processor circuits. The second stage manual bypass circuit has been retained, and isolated, in order to reduce the probability of a system failure should a failure occur in the second stage regulator. Furthermore, 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 servo-valves for automated oxygen partial pressure control.

The next step involves the construction of a parallel processor output system (right half, Fig. 11). 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 "third's" 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.

The system survival probability for the redundant rebreather is approximately 41times greater than that for existing mixed-gas rebreathers. The mission failure

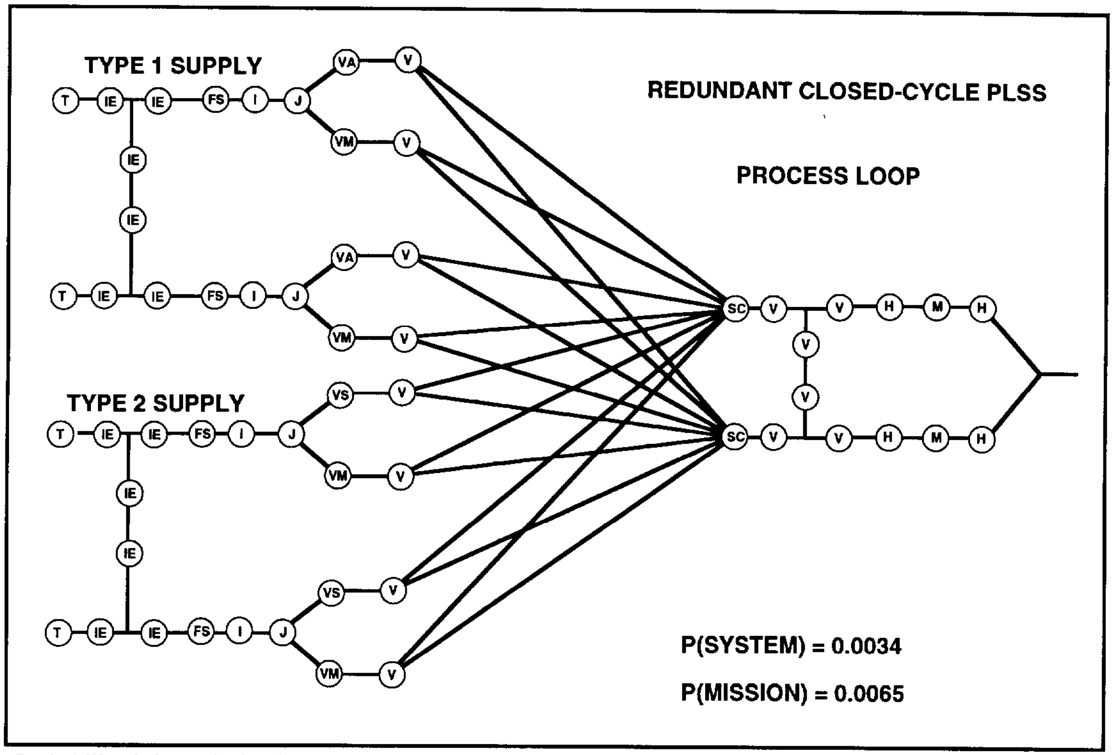

Fig. 11: Probability Schematic for the MK1 Mixed Gas Rebreather, used in December 1987 to conduct a 24-hour continuous underwater mission at Wakulla Springs, Florida. Only half of the consumables were expended during that time period. The device weighed 91 kg (200 lb) dry and was neutrally buoyant underwater. It utilized anhydrous lithium hydroxide as the carbon dioxide removal agent and operated under the control of four onboard computers.

probability is 20 times lower than that for a simple Bi-linear open-circuit architecture, which is significant considering that the mixed gas system is substantially more complex and offers vast improvements in range. There is no comparison with existing naval rebreathers, nor government spacesuits on a mission failure basis, since none are redundant. To summarize the key points of the above discussion:

1. System failure probability can be decreased by providing multiple, independent life support subsystems (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 failure probability in proportion to the product of the individual path failure probabilities. However, field experience has shown that system management becomes excessively task-loaded 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. Q/A attention needs to be focused on the isolation elements.

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.

Developing Practical Redundant PLSS Backpacks:

Several generations of redundant closed-cycle PLSS systems based on the architecture depicted in Fig. 11 have been implemented by Cis-Lunar Development Laboratories, Inc.* since 1987. The MK1 bore the unusual distinction of being used to conduct the first continuous 24-hour duration dive conducted by an individual equipped only with a backpack PLSS. By 1993 the third-generation unit, the MK3, was developed using

---

* Any mention of commercial products is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

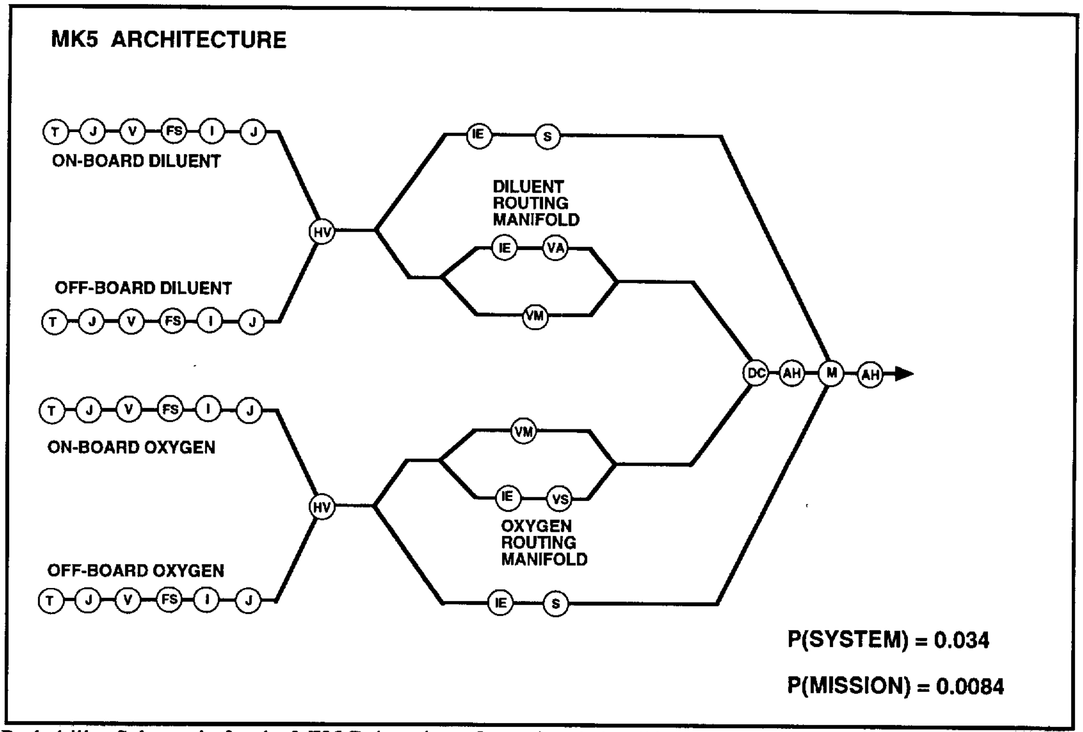

Fig. 12: Probability Schematic for the MK5 Rebreather. Operational simplifications have been made in the cross-connect areas to utilize a Hi-Rel switching valve (HV) which is used to route low pressure gas supplies. The capacity of the HV diverter is six times the maximum charging pressure of the supply gas tanks. In the oxygen and diluent routing areas, redundant, isolated output paths have been enabled, including the ability to access, in open-circuit mode, all gas supplies in the PLSS. Dual seals and exterior "armor" have been used to reduce failure probability in the process loop. Range is 6-10 hours in a 32 kg pack.

an architecture identical to that shown in Fig. 11, but in a much more compact device. It consisted of twin 8-hour closed-cycle systems and weighed approximately 55 kg. For typical cave diving exploration missions the device was augmented with a 3000 liter composite open circuit bailout cylinder as a tertiary independent supply. The lessons applied to the mechanical systems were also applied to the electronics control systems. Three onboard computers were used to automatically monitor and control oxygen partial pressure, measure carbon dioxide levels, tank pressures, and ambient pressure (depth). Computer-driven head-up displays provided critical system and sensor feedback through-the-mask, while a menu-driven, interactive, LCD display allowed for both system status and error messages to be displayed as well as for the user to override system control presets (e.g. PPO2 setpoint, inert gas select etc.).

The embedded computer architecture was such that any of the three independent processor units could control the entire device, even if others had dropped out. Each computer had an independent power supply. Beyond this, an entirely independent control system was implemented which consisted of a direct sensor-driven oxygen partial pressure display and manual gas injection panel. This permitted reliable operation of the device even in the event of a three-way power crash in the computer control system.

Field experience on these units began to reveal human-factors problems as early as 1989. The dual closed cycle backpack had two mouthpieces, two HUDs, two LCD displays, two backup PPO2 displays, two manual control panels, and two auxiliary open circuit regulators for mission aborts. In addition to this, on a typical long range cave dive one rides an electric propulsion vehicle (at velocities of 1 to 1.5 m/s), must carry a high intensity (multiply redundant) lighting system (since there is no ambient light), and must run a large reel of guideline (since silting can reduce visibility to zero and obscure the way out). Despite significant efforts to segregate all this gear (System 1 and System 2 labels, left and right-handed hardware etc.) task loading became overwhelming and the bulk of dual closed-cycle PLSS's within a single backpack made for awkward going. Similar arguments (environment specific) apply to EVA PLSS task loading.

As a result, a re-assessment took place in 1993 in an effort to trim the size of the backpack. The result of this effort is shown in Figure 12. It was observed, over the course of thousands of hours of use, that the ambient

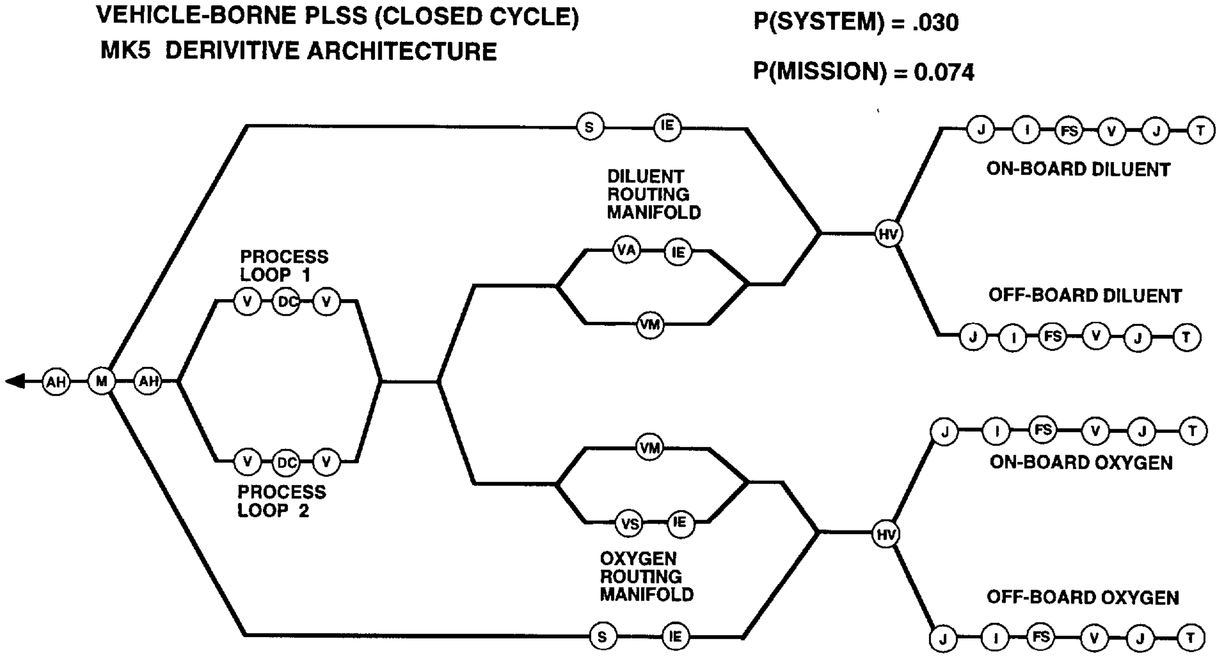

Fig. 13: Probability Schematic for Vehicle-Borne, Extended Range MK5 System Under Production for the Wakulla 2 Project. The range is 12 to 20 hours, depending on individual user metabolism. Although two carbon dioxide processors are available, only one breathing loop subsystem is used in order to decrease user task loading.

pressure portions of the system (i.e. the process loop) had never suffered a failure. There had been numerous malfunctions typically anticipated of an electromechanical system in a mature state of use: occassional regulator failures and occassional power crashes in the automatic control system. A strategy was thus adopted, for the mission specific objective of charting an unexplored underwater tunnel beginning at a depth of 1325 meters vertically below the surface of Mexico's Huautla plateau[8], to maintain full redundancy only in those subsystems that had shown propensity to fail, while using a single process loop with enhanced reliability (i.e. greater MTBF). This was done, e.g., by using armored hoses contained within exterior ballistics abrasion-proof shells (to prevent catastrophic severing from sharp objects); by developing techniques to purge water from the carbon dioxide processor; and by implementing high reliability (hi-rel) switching valves between the various gas supplies. This approach was used successfully to decrease mission failure probability in the context of a compact, simple user-interface backpack. The sacrifice made was in the achievable range of the device: the maximum outbound time was limited by the open circuit bailout gas carried, since we still had to deal with the possibility of a system failure in the process unit at the point of maximum distance from base. This amounted to one hour at 30 m water depth, or approximately a one kilometer exploration radius.

During the actual project 22 missions were carried out with average outbound ranges of 600 m and durations of approximately 80 minutes for one-way transit. This range (which exceeded the duration of the bailout system) was made possible by using staged open-circuit PLSS units which were suspended from the guide line at the mid-point of the underwater tunnel. None of these "stage bottles," nor the open circuit bailouts carried by each explorer, were ever used. One first stage regulator (there were six in each backpack) failed due to grit in the diaphram but was detected during a pre-dive inspection and was replaced on site. One depth pressure sensor failed due to human error during a calibration procedure and was replaced on site. During the return from the final mission a bulkhead oring failed on an LCD display (due to a retainer nut loosening under shock loading sustained during transport) allowing water to enter and short the display and its local CPU. The remaining two processors (located in independent cases) voted the non-responding computer out of the loop and took control of the system. Information con-

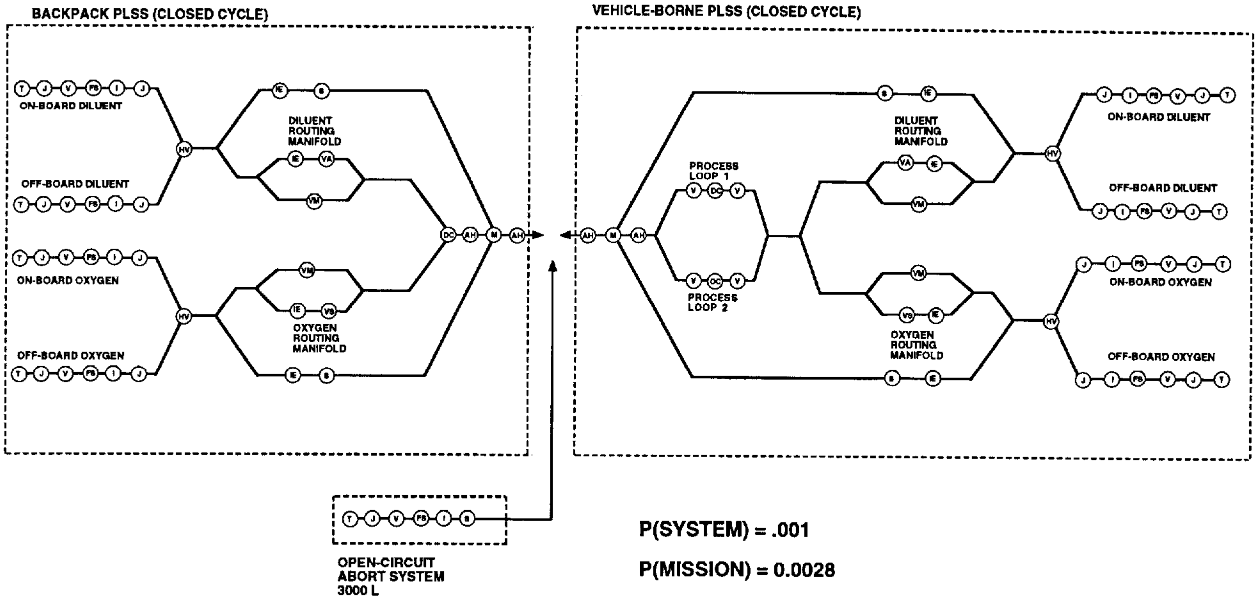

Fig. 14: Wakulla 2 PLSS System. In order to increase range and decrease operator task loading, two independent closed cycle PLSS units were designed, each containing internal redundancy. The vehicle-borne unit's range was extended through the use of parallel process sub-systems, either of which, or both, can be selected for use. The backpack PLSS is only used for abort scenarios, which account for complete loss of the primary vehicle and its onboard PLSS system.

cerning system status, PPO2 etc. remained accessible via the HUD and backup display systems.

The Wakulla 2 project[9], scheduled for October - December 1997, has as its objective the charting of unknown galleries inside Wakulla Springs, Florida to outbound distances of 6 kilometers from the entrance at 100 meter water depths. These parameters, driven largely by exploration curiosity, completely change PLSS design criteria. Although the outbound leg is anticipated to be achieved in approximately 120-150 minutes using electric propulsion vehicles, the abort leg PLSS requirements must be predicated on a redundant failure of the propulsion vehicles (each explorer carries two, one in front, one towed behind) at the point of maximum outbound range. A swimming diver can be expected to achieve 0.3 m/s, giving a return time of 330 minutes. Together this amounts to 480 minutes (8 hours) of life support, not counting the reserve supplies described above. With a 4:1 reserve ratio, a total of 32 hours of life support are needed. This cannot be accomplished using open circuit bailout systems.

In order to achieve these requirements the architecture shown in Fig. 14 was developed. In this design a second closed-cycle PLSS unit is housed in a strap-down contoured shell that mounts on the towing propulsion vehicle. By placing the PLSS on the vehicle itself, the human-factors problems of the redundant backpack are eliminated -- the second unit is self-contained and readily accessible in front of the user with no possibility for mixup of system peripherals, and where feedback displays can be optimally positioned for viewability and ease of access. Two important additional advantages arise from this architecture:

1) Dual, selectable, carbon dioxide processing stacks can be placed on the vehicle with minimal increase in profile drag. These further increase both range and system reliability. Each of the dual oxygen and diluent gas supplies provides enough gas to drive both CO2 processors to completion at approximately 20 hours maximum range.

2) Because the primary life support system is contained on the vehicle, it can be ditched in an emergency, leaving the explorer with what amounts to the original system described above that was used in Huautla: a 6-10 hour slim profile backpack with an additional 1 hour open circuit abort bottle. This lower profile permits a faster return on the abort vehicle since drag is significantly reduced.

Since each PLSS described above can tolerate at least two major sub-system failures before being rendered dysfunctional, this architecture amounts to a "fail-operational; fail-operational; fail-safe" system.

Concluding Remarks:

The above concepts bear directly on EVA PLSS considerations. Bulk (inertia) and human factors are essentially the same whether you are neutrally buoyant underwater or weightless in orbit. A lightweight, open exoskeleton-based sit-down or stand-up, medium to long range, orbital manned maneuvering vehicle can be developed along these lines. This approach obviates the need for complex backmounted MMU's and allows you to bring more of what you need to a remote work site (perhaps several hours from an orbiting industrial facility). This is a close analog to procedures now used for saturation commercial diving, where umbilicals from a transfer capsule are used for the primary life support while each worker has a slim, back-mounted secondary system for mission aborts. The same should be true in orbit or on the moon. The connections to the spacesuit from the "offboard" PLSS can be accomplished in much the same fashion as was used for Apollo lunar EVAs, using two umbilical snap-to-connect hoses.

There are, of course, many fine points concerning spacesuit PLSS design not addressed here. Thermal and humidity control systems must also be included. Forced air drive systems and power supplies are needed. Reliability Q/A is still an issue for the suit shell, since it represents an unavoidable linear system. But the most complex components -- which comprise the PLSS -- can be addressed from a different perspective, in that less costly, but multiply redundant, systems can be employed. As a measure of the cost reduction that might be achieved, the off-the-shelf Cis-Lunar MK5 backpack, which is a fully closed-cycle system operating under redundant computer control with a range of 6 to 10 hours (depending on user metabolic rate) at 230 meters underwater with gas mixture control capabilities and onboard real-time decompression, retails commercially for $15,000 U.S. From this, it is not a great leap of the imagination to conceive of the development of a fully redundant closed-cycle industrial spacesuit for $250,000.

References:

[1] Stone, W.C. Ed., Reducing the Cost of Space Infrastructure and Operations, Part 1, NISTIR 5255, NIST, Gaithersburg, MD, 1993, 199 pp.

[2] Dhillon, B.S., Systems Reliability, Maintainability and Management, Petrocelli Book, New York. 1983. pp. 71-90.

[3] Billinton, R. and Allan, R.N., Reliability Evaluation of Engineering Systems: Concepts and Techniques, Plenum Press, New York,1983. pp. 282-301.

[4] Nash, F.R., Estimating Device Reliability: Assessment of Credibility, Kluwer Academic Publishers, Boston, 1993. pp. 23-27.

[5] Ireson, W.G., and Coombs, C.F. Jr., Handbook of Reliability Engineering and Management, McGraw-Hill, New York, 1988. pp. 19.37-19.39

[6] Lewis, W.C., LSA for Mars Class Missions, Space Manufacturing 7, Proceedings, Ninth Princeton Conference, May 10-13, 1989, AIAA, Washington, DC. pp. 274-278.

[7] Stone, W.C., The Wakulla Springs Project, National Speleological Society, Huntsville, AL, 1989, 212 pp.

[8] Stone, W.C., Huautla Cave Quest, National Geographic Magazine, Vol. 188, No. 3, September 1995, pp. 78-93.

[9] http://www.wakulla2.com

[10] Stone, W.C., The 1984 Pena Colorada Cave Expedition, The Explorers Journal, The Explorers Club, New York, Vol. 63, No. 2, June 1985, pp. 58-69.