Methods and Costs to Achieve Ultra Reliable Life Support

Harry W. Jones[1]
NASA Ames Research Center, Moffett Field, CA, 94035-0001

A published Mars mission is used to explore the methods and costs to achieve ultra reliable life support. The Mars mission and its recycling life support design are described. The life support systems were made triply redundant, implying that each individual system will have fairly good reliability. Ultra reliable life support is needed for Mars and other long, distant missions. Current systems apparently have insufficient reliability. The life cycle cost of the Mars life support system is estimated. Reliability can be increased by improving the intrinsic system reliability, adding spare parts, or by providing technically diverse redundant systems. The costs of these approaches are estimated. Adding spares is least costly but may be defeated by common cause failures. Using two technically diverse systems is effective but doubles the life cycle cost. Achieving ultra reliability is worth its high cost because the penalty for failure is very high.

Nomenclature

4BMS	=	Four Bed Molecular Sieve
ALS	=	Advanced Life Support
AMCM	=	Advanced Missions Cost Model
B	=	Benefit
C	=	Cost
C(F)	=	Cost depending on F
CER	=	Cost Estimating Relationship
CM	=	Crewmember
Co	=	original Cost
D	=	Duration, Damage
DDT&E	=	Design, Development, Test, and Evaluation
E	=	rocket Exhaust speed
ECLSS	=	Environmental Control and Life Support System
EM	=	Equivalent Mass
ESM	=	Equivalent System Mass
EVA	=	Extravehicular Activity
F	=	Failure probability
F dual	=	Failure probability for two dual redundant parallel strings of N components
F single	=	Failure probability for one single string of N components
FMEA	=	Failure Modes and Effects Analysis
Fo	=	original Failure rate
go	=	acceleration of gravity
HEO	=	High Earth Orbit
Isp	=	specific Impulse
ISRU	=	In Situ Resource Utilization
ISS	=	International Space Station
JSC	=	Johnson Space Center
LCC	=	Life Cycle Cost
LEO	=	Low Earth Orbit
LOC	=	Loss of Crew
LOM	=	Loss of Mission

[1] Systems Engineer, Bioengineering Branch, Mail Stop N239-8, AIAA Senior Member.

LSS = Life Support Systems
M = Mass
Mt = total initial Mass
MTBF = Mean Time Before Failure
MTTR = Mean Time To Repair
Mv = vehicle Mass
N = Number of units
NAFCOM = NASA-Air Force Cost Model
NRC = National Research Council
OGA = Oxygen Generation Assembly
P = Propellant mass
PHA = Preliminary Hazard Analysis
PRA = Probabilistic Risk Assessment
R = Reliability. mass of the rocket
RAM = Reliability, Availability, and Maintainability
S = payload System mass
TCCS = Trace Contaminant Control System
VCD = Vapor Compression Distillation
Δv = delta-v, change in velocity
λ = Lambda, failure rate

I. Introduction

THIS paper attempts to define the best approach to achieve ultra reliable recycling space life support systems, by considering alternate reliability methods and their costs. Humans on long duration missions such as the space station consume large amounts of oxygen and water. Recycling is required to reduce the launch mass and cost. Distant missions such as Mars exploration have long travel time and, if a failure occurs, cannot quickly obtain life support materials or spare parts or bring the crew home. Ultra reliable recycling life support is needed, and it has yet to be developed and demonstrated. Distant missions must perform cost-effective exploration with assured high probability of a safe crew return.

The analysis uses an example Mars mission to establish the life support system design and the expected reliability. The life support costs and the standard reliability approach are described. Then the methods and costs to achieve ultra reliable life support are considered.

The paper is organized as follows:

1. Example Mars mission and life support system
2. Mars ECLSS reliability
3. Ultra reliability is needed for long, distant missions
4. ECLSS mass, volume, power, and cooling
5. ECLSS Life Cycle Cost (LCC)
6. Design for ultra reliability
7. Costs of improving reliability
8. How much reliability is cost effective?

II. Example Mars mission and life support system

A classic Mars mission plan is described. The life support reliability requirements and approach are discussed and the life cycle cost is estimated.

A long, distant mission such as Mars exploration requires ultra reliable recycling life support for the transit to and from Mars and the long stay on the surface. The surface system will have several advantages over the transit system, including operation in gravity and access to atmospheric resources, but it will have to deal with potential contamination by surface dust, variable oxygen and water demands due to Extravehicular Activity (EVA), and possible impacts of the daily light and thermal cycle.

The big-picture overview digest, Human Spaceflight: Mission Analysis and Design, considers the major aspects of designing human space missions in specialized chapters. (Larson and Pranke) A lunar base example is developed throughout the book to illustrate the detailed processes. A Mars design example forms the final chapter.

A. The Mars mission

Connolly provides the Mars example reference mission and life support design used here. (Connolly) The many mission requirements reflect scientific, programmatic, and human needs. The requirements directly related to life support reliability are:

> "Have life-critical systems that are two-fault tolerant,
> Maintain reliability by making systems simple, redundant, inter-changeable, and maintainable, and,
> Use closed, highly maintainable systems." (Connolly, p. 982)

The first requirement is a rigorous design practice that can be verified by analysis, but the second and third are good advice rather than verifiable requirements. There are no quantitative requirements for reliability or probability of Loss of Crew.

The crew size is assumed to be six. A conjunction class, long surface stay mission was chosen, with a 75 metric ton shuttle-derived launcher. Mars surface elements are predeployed in a split multi launch mission. Solar electric propulsion is used to ferry cargo slowly from Low Earth Orbit (LEO) to High Earth Orbit (HEO) where the Mars vehicle is assembled. The crew later joins using a small fast ascent vehicle. More than the minimum amount of chemical propellant is used to achieve a 180 day transit to Mars, which is faster than the minimum energy Hohmann orbit of about 235 days. The Mars ascent rocket propellant will be produced on Mars from in-situ resources before the crew leaves Earth.

A detailed design is provided for the habitat-lander, which takes the crew from HEO to the Mars surface and then serves as the core habitat. The habitat-lander uses aerobraking during descent. An ascent vehicle later takes the crew to the Earth return vehicle which was predeployed in Mars orbit. The crew will spend 180 days in transit and 500 days on the surface. A predeployed inflatable surface laboratory and solar power grid are attached to the habitat lander on the surface.

B. ECLSS reliability requirements

The habitat lander ECLSS (Environmental Control and Life Support System) is described. "(T)he ECLSS is central to the crew's … survival. It must work from the moment the crew boards the vehicle …, through the six months coast in 'zero-g,' and then for 500+ days on the Martian surface." (Connolly, p. 994) "Choosing an ECLSS therefore actually means choosing the system's level of closure and a strategy for redundancy or maintainability to make the system nearly 100% available." (Connolly, p. 994) Water and oxygen can be predeployed on the Martian surface or produced from the Martian atmosphere, but these resources are not available in transit to Mars, "so we must design the ECLSS to protect from all credible failures during this phase." (Connolly, pp. 994-5)

In addition to the mission level requirements, here are two more reliability requirements specifically for ECLSS, "nearly 100% available," and "protect from all credible failures." The second is less stringent than the earlier mission level requirement, "Have life-critical systems that are two-fault tolerant," which was apparently loosened to single fault tolerant for ECLSS, as seen in the use of only 2x redundancy below.

(The requirement definition of "nearly 100% available" is questionable. Suppose ECLSS was 99.8% available. It would not be available on one of the 500 days on the surface. Nearly 100% crew survival is what we want.)

C. ECLSS design and redundancy

Connolly uses an ECLSS design from the ECLSS chapter in Human Spaceflight: Mission Analysis and Design. (Doll and Eckart) The ECLSS includes a four bed molecular sieve (4BMS) for carbon dioxide removal, a trace contaminant control system (TCCS), an electrolysis oxygen generation assembly (OGA), and vapor compression distillation (VCD) to purify water condensed from the atmosphere. Solid waste is not recycled. (Connolly, p. 995)

The food is hydrated, with about 1 kg per crewmember per day of water that can be used to make up any recycling losses. (Connolly, p. 997) For six crew and 180 + 500 days total duration, the food provides 4,080 kg of water.

Reliability is provided by full system redundancy. Two spares, 3x redundancy, are provided for the 4BMS, TCCS, and OGA. One system spare, 2x redundancy, is provided for the apparently less critical VCD. (Connolly, p. 998)

III. Mars ECLSS reliability

Since the crew can respond to failures, a crewed spacecraft can be designed as a repairable system. The JSC Human-Rating Requirements state that no single failure shall cause loss of life or vehicle and that analysis can assume that the crew can repair the failure. (Heydorn and Railsback, p. 195) This requires 2x redundancy or a full

set of spares. Connolly's Mars design example uses full system redundancy for reliability. In addition to the ECLSS subsystem redundancy, the habitat/lander has dual airlocks and three spare EVA suits. (Connolly, p. 998)

As usual for life support, reliability is not specifically considered in the ECLSS design chapter of Human Spaceflight, but it notes "A real design would require system redundancy based on risk analysis." (Doll and Eckart) Loss of life support is listed as a major hazard to be analyzed in the chapter on safety. (Heydorn and Railsback)

A. Implicit ECLSS reliability

Connolly's Mars design example does not specifically estimate the ECLSS reliability, but the level of redundancy used does suggest a number. His discussion emphasizes that the 180 day transit is the most dangerous time, since stored and ISRU produced oxygen and water will be available after landing on Mars. And costly additional propellant is used to reduce the Mars transit time from 235 to 180 days. The design provides triple redundancy for three of the four ECLSS systems, and double redundancy for the fourth.

Triple redundancy suggests that the assumed probability that an ECLSS subsystem, such as the 4BMS, will fail on the 180 day transit is on the order of 0.1, ten percent. The probability that two redundant subsystems both fail is then 0.1 * 0.1 = 0.01, or one percent, which seems too high considering that there are four different subsystems that probably will have a similar failure probability. The probability that three redundant subsystems all fail would be 0.1 * 0.1 *0.1 = 0.001, or one in a thousand. Double redundancy is not enough, but triple redundancy is sufficient to keep the total probability failure of any one of the four ECLSS subsystems to 0.004, or 0.4 percent.

If the subsystem failure probability was an order of magnitude lower, 0.01, one percent, the probability that two redundant subsystems both fail would be 0.01 * 0.01 = 0.0001, or one in ten thousand, and there would be no need for triple redundancy. If the subsystem failure probability was much higher, 0.3, 30 percent, the probability that three redundant subsystems all fail would be 0.3 * 0.3 *0.3 = 0.027, 2.7 percent, and triple redundancy would not be enough.

This shows that the implicit estimated probability that an ECLSS system would fail on a 180 day mission is roughly 0.1, corresponding to a failure rate of 0.1/180 days = $5.5 * 10^{-4}$ per day. This is equal to one failure in 1,800 days or 4.9 years. To verify this failure rate, it would be necessary to have several years of operations without a failure. To accurately measure this low failure rate, it would be necessary to run several units until failure, which could easily take ten years.

The low implicit failure rate means that the ECLSS is expected to have reasonably good reliability. But even with the assumed good reliability, it was thought necessary to provide triple ECLSS redundancy, a shortened transit, and waiting surface life support resources and systems to reduce the probability of losing of life support.

B. Recommended qualitative high level reliability approach

Reliability analysis and design is described in the "Safety of Crewed Spaceflight" chapter of Human Spaceflight: Mission Analysis and Design. (Heydorn and Railsback) Some important general statements are as follows: "The ideal design is simple and made of safe components." "Redundancy can place large demands on maintenance … and add considerably to the structure's mass and volume." "We can use statistical methods to develop safety measures that can be evaluated with other performance measures." "We'll summarize qualitative measures … to identify hazards and analyze failure modes and effects. These methods are part of our quantitative analysis, which blends probabilistic risk assessment (PRA) and analysis of statistical reliability." And, "A crewed spacecraft can be designed as a repairable system by using the crew to lessen failure effects."

The two important qualitative safety methods are preliminary hazard analysis (PHA) and failure modes and effects analysis (FMEA). PHA starts with a potential hazard, such as a fire, and asks what could cause it to happen. PHA is top-down and deductive, sometimes using fault trees. FMEA starts with the parts list and schematic and asks if this part fails, what hazard might it cause. FMEA is bottom-up and inductive. PHA and FMEA together should provide a full and consistent picture of all the failure causes and hazard effects.

C. Alternate quantitative reliability approach

For a quantitative analysis, the key requirement is the Probability of Loss of Crew (LOC) during the mission. The probability of LOC is computed using a reliability block diagram and the system and subsystem failure rates. The failure rates ideally are based on test data, but they may be estimated from similar systems in a database. The probability of LOC can be reduced by adding redundancy. The uncertainty and distribution of the reliability estimate should be considered, possibly by defining the 90 percent confidence interval. Additional failure data reduces the reliability uncertainty and reduces the need for redundancy. Common cause failures can limit the reliability gains from redundancy.

IV. Ultra reliability is needed for Mars and other long, distant missions

It is well accepted that higher reliability and onboard repair will be required for deep space, the Moon, and Mars.

> The factors of reliability and maintainability will assume immense importance as U.S. human spaceflight advances to extended operations in deep space, on the lunar surface, and on Mars. There will be no rapid return capability; resupply will be slow, difficult, and expensive; refurbishment now accomplished on the ground will have to be accomplished on site. (NRC, p. 77)

Long duration, short distance missions such as the space station or a permanent moon base can depend on frequent resupply. Spares can be provided when a failure occurs. In an emergency, the crew can return to Earth. For long distance, long duration missions, providing emergency spares or crew return is not possible. All the necessary equipment must be provided as part of the mission.

To achieve the required overall mission reliability, all the major mission elements such as life support must be an order of magnitude more reliable than the entire mission. If the mission requirement is 1 in 1,000, life support must have only roughly a 1 in 10,000 probability of failure over the mission duration.

The life support reliability requirement flows down to the component level. Suppose that life support has ten individual life support systems, each with ten subsystems, and that each subsystem has ten components. Life support then has a total of one thousand components. Assume that each component has a failure rate of F failures per hour. The probability of a life support system failure is then 1,000 * F failures per hour. Suppose further that the mission duration is 10,000 hours (1.1 years) and that the total life support failure probability must be no more than 1 in 10,000. To achieve this, the component failure probability must be such that 1,000 * F failures per hour * 10,000 hours < 0.0001. This requires a component failure rate of $F < 10^{-11}$ failures per hour. Such extremely reliable components are not available for most life support applications. To expect to observe one failure in a component with 10^{-11} failures per hour, it would be necessary to test one million units for 11 years (100,000 hours), or another number and duration with an equal number of unit-hours.

A. Current life support systems apparently have insufficient reliability

Current recycling life support systems do not appear to have the ultra reliability required for long missions, which is much higher than that needed for near Earth short duration missions such as the International space Station (ISS)

Likens noted that actual life support failure rates have been significantly greater than predicted. The predicted failure rates ranged from $3 * 10^{-4}$ to $3 * 10^{-5}$ per hour, a one order of magnitude range. However, the actual failure rates ranged from 10^{-1} to 10^{-5}, a four orders of magnitude range. Almost always, with only one exception in fifteen cases, the actual failure rates were higher than the predicted. They were usually a full order of magnitude higher. Storage, resupply, and non-recycling technologies were found to be significantly more reliable than physical-chemical water processors. Only failure mitigation using emergency oxygen and water reserves or repair and work-arounds was able to prevent disaster. (Likens)

Russell and Klaus state for the space station that "total ECLSS maintenance for 865 days was found to exceed the design estimate by a factor of 22." A contributing factor was the oxygen generation system's greater than expected failure rate. (Russell and Klaus) William Gerstenmaier, NASA's associate administrator for space operations, expected this failure cause to continue on the International Space Station. "We know that oxygen generating systems in general have a lot of problems over the years during start-up. We think we'll have some problems with our oxygen generator system." (Malik)

A Valador report estimated the failure rates for thirty-two different components of the life support system, in the air revitalization, atmosphere and pressure control, and water recovery and management subsystems. The failure rates were $1.43 * 10^{-4}$ or lower. The life support system failure rate is the sum of all the component failure rates, which was $5.71 * 10^{-4}$ per hour. (Ramamurthy et al., p. 32) This failure rate corresponds to a Mean Time Before Failure (MTBF) of 1,750 hours or 73 days. If the mission duration is 10,000 hours (1.1 years), $5.71 * 10^{-4} * 10^{4} = 5.71$ failures are expected over the mission.

V. ECLSS mass, volume, power, and cooling

Table 1 shows the mass, volume, power, and cooling requirements per crewmember (CM) of the ECLSS subsystems. (Doll and Eckart, pp. 554, 558)

Table 1. Mass, volume, power, and cooling of the ECLSS subsystems.

	Mass kg/CM	Volume m^3/CM	Power kW/CM	Cooling kW/CM
4BMS	30	0.15	0.30	0.30
TCCS	20	0.15	0.05	0.05
OGA	35	0.03	0.35	0.10
VCD	25	0.10	0.03	0.03

The ECLSS is similar to that of ISS, but does not include the ISS's Sabatier carbon dioxide reduction, multifiltration wastewater processing, and oxygen and water storage tanks. Including these would multiply the mass per crewmember by a factor of five. Allowing for ISS racks and packaging would cause a further doubling of the mass per crewmember. (Jones, 2007-01-3221)

A. ECLSS Equivalent System Mass (ESM)

Table 2 uses the mass, volume, power, and cooling requirements of the ECLSS subsystems to compute the Equivalent System Mass (ESM) of the Mars ECLSS, for six crew and the 3x and 2x redundancy factors.

Table 2. ESM of the Mars ECLSS for six crew with redundancy.

	Mass, kg	Volume, m3	Volume ESM, kg	Power, kW	Power ESM, kg	Cooling, kW	Cooling ESM, kg	ESM, kg
Mass equivalent			42.4 kg/m^3		39.6 kg/kW		30.2 kg/kW	
4BMS (3x)	540	2.70	114.48	0.30	11.88	0.30	9.06	675
TCCS (3x)	360	2.70	114.48	0.05	1.98	0.05	1.51	478
OGA (3x)	630	0.54	22.90	0.35	13.86	0.10	3.02	670
VCD (2x)	300	1.20	50.88	0.03	1.19	0.03	0.91	353
Totals	1,830	7.14	302.74	0.73	28.91	0.48	14.50	2,176

All the requirement numbers in Table 1 are multiplied by six for the six crewmembers. The required mass and volume are tripled or doubled for the redundancy factors, but not the power and cooling, since only one set of ECLSS systems will be in operation while the redundant units are stored as backups in case of failure.

The ESM of a system is the sum of the mass of the hardware and its required spares, and of the pressurized volume, power supply, and cooling system needed to support the hardware in space. The ESM is the total launch mass needed to provide and support the system. ESM = Mass + Volume*mass equivalent of volume + Power * mass equivalent of power + cooling * mass equivalent of cooling.

The mass equivalent of volume is found by dividing the mass of the spacecraft by its internal volume, thus obtaining the mass required to provide a cubic meter of the pressurized volume required to house the ECLSS. The spacecraft structure and mechanisms require 15,256 kg to provide 360 m^3 of pressurized volume, for 42.4 kg/m^3. The mass equivalent of power is the power supply mass divided by the power supply capacity in Watts, 25 kW requiring 990 kg, or 39.6 kg/kW. The mass equivalent of cooling is the thermal cooling system mass divided by its cooling capacity in Watts, 25 kW requiring 754 kg, or 30.2 kg/kW. (Connolly, p. 998)

The hardware mass accounts for 84 percent of the ESM and the mass equivalent of volume for 14 percent, so that the power and cooling needs are negligible, only 2 percent of ESM. The total habitat-lander dry mass is 45.3 metric tons, so the ECLS ESM is only 4.8 percent of the total mass. (Connolly, p. 998)

VI. ECLSS Life Cycle Cost (LCC)

Life Cycle Cost (LCC) includes all the costs incurred during the development, launch and emplacement, and operations phases of a space mission.

A. Development cost

Development cost includes DDT&E (Design, Development, Test, and Engineering) and hardware production. Development cost can be estimated using the Johnson Space Center (JSC) Advanced Missions Cost Model (AMCM). The model is a single equation using mass, quantity, mission type, number of design generations, and technical difficulty to estimate the total cost for DDT&E and production.

The AMCM cost in millions of 1999 dollars is:

$$\text{Cost} = 5.65 * 10^{-4}\, Q^{0.59}\, M^{0.66}\, 80.6^{T}\, (3.81 * 10^{-55})^{(1/(Y-1900))}\, G^{-0.36}\, 1.57^{D}$$

Q is the total quantity of development and production units, M is the system dry mass in pounds, T calibrates for the type of mission (2.13 for human habitat, 2.46 for crewed planetary lander), Y is the year of initial operation, G is the hardware generation (1 for new design, 2 for second generation), and D is the estimated difficulty (0 for average, 2.5 for extremely difficult, and -2.5 for extremely easy). (Guerra and Shishko, pp. 946-7) (AMCM)

If the quantity is ten to include redundant, test and prototype units, the total single system ECLSS mass is 110 kg (242 pounds), the mission is crewed planetary lander (T = 2.46), 2020 is the year of initial operation, the design is second generation based on space station, and the difficulty is average (0), the estimated cost is 1.12 billion dollars, 1 million dollars per kilogram for the Mars mission.

For a human space habitat (T = 2.13), 2000 the year of initial operation, low difficulty (D = -2), and all else unchanged, the estimated cost is only 87 million dollars, 79 thousand dollars per kilogram. This is similar to International Space Station (ISS) costs. The development and production cost for human missions is typically $100 k/kg, with a range of from $50 to 150 k/kg. (Wertz and Larson, p. 254) (Guerra and Shishko, p. 953)

Costs are much higher for planetary missions than for Earth orbit missions. This is partly due to the need for higher performance and reliability, but also because of the much higher emplacement cost per kilogram for planetary missions. The effort of reducing system mass for distant missions increases the total DDT&E cost and so the DDT&E cost per kilogram increases even faster. Reducing the mass reduces the emplacement cost, with the objective of minimizing total mission cost. We next consider launch and emplacement cost.

B. Launch and emplacement cost

The Space Shuttle cost to launch to LEO is typically quoted as $25 k/kg. (Wertz and Larson, p. 125) A yearly Space Shuttle budget of 4 billion dollars for 10 launches of 16,000 kg to LEO corresponds to a cost of $25 k/kg. Actual recent costs are much higher due to many fewer launches. An incremental cost per launch of 1.2 billion dollars corresponds to a three times higher cost of $75 k/kg. (Pielke and Byerly) The traditional cost of $25 k/kg is used here.

For a Mars mission, we must launch to LEO the payload and the propulsion system - the vehicle and propellant - needed to get the payload to the planetary surface. For a Mars landing, the stack-to-payload mass ratio is roughly 12, derived below. This suggests launch and emplacement costs will be about $300k/kg. The launch and emplacement cost applies to the total life support mass of 1,830 kg, for a total cost of 549 million dollars.

The launch cost per kilogram for a planetary mission is about 30 percent of the payload development cost per kilogram, not much larger as sometimes assumed. The high total cost is not unexpected. “The cost of a human-crewed mission to the Moon or Mars is typically millions of dollars per delivered kg.” (Wertz and Larson, p. 254)

C. Stack-to-payload mass ratio

The Mars surface life support system must be accelerated to LEO, then on to Mars, decelerated into Mars orbit, and descended to the Martian surface. The Δ v from LEO to Mars orbit and down to the surface is 4.9 km/s. No Mars orbit insertion or descent Δ v is included since aerocapture and aerobraking will be used, not propulsion, but some propulsion Δ v is included to adjust the landing site. (Condon et al., pp. 277-278)

The rocket equation shows that the ratio of the total rocket mass to the payload vehicle mass increases exponentially with the required Δ v. Mt/Mv = exp (Δ v/E), where Mt is the total initial mass of the rocket propulsion system and fuel plus Mv, the vehicle mass, exp is the exponential function, Δ v is delta-v, the total required change in velocity, and E is the rocket exhaust speed. (E = go Isp, go = 9.8 m/s^2 and Isp is the specific impulse, assumed equal to 320 s, so E = 3.14 km/s.) (Condon et al., p. 276) For a Δ v of 4.9 km/s from LEO to Mars orbit and down to the surface, Mt/Mv = 4.8.

The actual total launch to payload mass ratio is significantly higher, since the final vehicle mass Mv includes the mass of the rocket engine and fuel tank, R, as well as the payload system mass, S. Mv = R + S. Mt includes the propellant mass, P, plus the vehicle mass, Mv. Mt = P + Mv = P + R + S.

The stack-to-payload mass ratio is Mt/S. It can be calculated from the mass ratio including the rocket, Mt/Mv = exp (Δ v/E) = (P+R+S)/(R+S), and the ratio of the rocket mass to rocket plus propellant mass, R/(R+P), estimated as 0.17. (Humble, pp. 772-3)

Mt/S = {Mt/Mv} [(1 - {R/(R+S)}]/[1 - {Mt/Mv}*{R/(R+S)}]

This equation can be derived from (Humble, pp. 769-70) with some manipulation. From LEO to Mars orbit and down to the surface, Mt/S = 11.9.

D. High launch cost leads to high development cost.

A simple example shows how a high launch cost per kilogram forces an increase in the development cost per kilogram. Suppose a system costs 10 million dollars to develop and weighs 100kg, so that the development cost is

$100k/kg. Suppose the mission launch and emplacement cost is $300k/kg. It pays to increase development cost to reduce mass until the cost of removing the last kilogram reaches $300k/kg. Suppose that we reduce the mass from 100 kg to 50 kg at an average cost of $150k/kg saved. The total development cost is the original 10 million plus 50 kg * 150k/kg = 7.5 million for mass reduction, or 17.5 million. The final development cost per kilogram is 350k/kg, for the last remaining 50 kg.

E. Design example launch and emplacement cost

Connolly's Mars design example uses solar electric propulsion to ferry cargo slowly from LEO to HEO where the Mars habitat/lander is assembled. Nuclear propulsion in LEO was ruled out. (Connolly, pp. 982, 986) A chemical rocket is used for a fast 180 day crew transit to Mars. The masses of the habit/lander and propulsion systems are shown in Table 3. (Connolly, pp. 987, 998, 999)

Table 3. Mars design example mass.

System	Mass, kg
Habtat/lander	45,284
Landing rocket, propellant, parachute	13,070
Transit power and thermal	980
Transit rocket, propellant, structure	1,700
Solar electric propulsion, with propellant	80,000
Total	141,034

The stack-to-payload mass ratio Mt/S = 3.1, much less than for conventional propulsion. This gives launch and emplacement costs of about 3.1 * $25 k/kg = $78k/kg. For the life support mass of 1,830 kg, the total cost is only 143 million dollars. The launch cost per kilogram for a planetary mission is only about 8 percent of the payload development cost per kilogram.

F. Operations cost

The operations phase of a human space mission begins when Earth orbit is achieved and continues until the crew is returned safely to Earth. Ground support provides constant coverage with on-call expertise for maintenance and trouble shooting. The system complexity (including software, monitoring and control, and different operational modes) and the mission duration are the major operations cost drivers.

Operations costs can be estimated as a percentage of development cost. ISS operations were estimated to cost roughly 11% of DDT&E per year, not including launch. (Guerra and Shishko, p. 938) The JSC Mission Operations Cost Model (MOCM) estimates the operations cost as a percentage of the total development and production cost of the spacecraft. For manned spacecraft, the estimated operations cost per year is 10.9% of the total development and production cost. (MOCM) (Jones, 2003-01-2635)

For a DDT&E cost of 1.12 billion dollars, an operations cost rate of 10.9 percent per year, and a mission of 180 + 500 days, the total operations cost is 227 million dollars.

G. Implications of life cycle cost

LCC includes development, launch and emplacement, and operations costs, which are shown in Table 4.

Table 4. ECLSS development, launch and emplacement, and operations costs.

Activity	Cost, $ millions	Percent
DDT&E	1,120	75
Launch and emplacement	143	10
Operations	227	15
Total	1,490	100

The ECLSS has mass of 110 kg for a single string, 1,830 kg including redundant units, an estimated development cost of 1.12 billion dollars, an estimated launch and emplacement cost of 143 million dollars for the design example, and an estimated operations cost of 227 million dollars. The total is 1.49 billion dollars, roughly 814k dollars per ECLSS kilogram.

The use of advanced solar/electric propulsion in the design example greatly reduced the habitat/lander launch and emplacement cost compared to standard rocket propulsion. This lower launch and emplacement cost has two important implications. First, extreme and expensive measures to reduce mass are not justified. The expenditure to remove a kilogram should be no more than the now much lower cost of emplacing that kilogram. Second, extreme

and expensive measures to improve single string reliability are not justified. Two and even three times redundancy is an affordable way to achieve operational reliability. There is less need for mass reduction and more need for high reliability than was long thought in life support systems research and analysis.

VII. Design methods and costs for ultra reliable ECLSS

Three different methods to improve reliability will be described. Component spares can be provided for on-board repair. Complete redundant systems using diverse technologies can be provided. Diverse systems are much more costly than component spares, but only they can prevent common cause failures. The intrinsic single-string reliability can be improved by repeated test and redesign. This is time consuming and difficult. Increasing intrinsic reliability is much more costly than providing component spares or even diverse systems.

VIII. The cost of improving reliability using spare parts

Using the most reliable available components is insufficient to achieve the needed life support reliability. Systems will fail. Life support for long duration missions, such as space station, a permanent moon base, or a Mars visit, can rely on the crew using spares or full systems to repair failures. Redundant or spare systems are used to mitigate the random failures remaining after development of reasonably reliable single string systems.

A simple calculation shows how system reliability increases when component spares are provided. Suppose that each component has a failure rate of F failures per hour and that the mission duration is D hours. The probability of any particular component failing over the mission duration is F D. If two parallel redundant components are provided, the probability that both will fail is $(F D)^2$, which is less than F D assuming that F D < 1. Suppose that the system has the number N of components. The probability that a system with one single string of N components will fail is F single = N F D. The probability that a system with two dual redundant parallel strings of N components will fail is F dual = N $(F D)^2$ = $(F single)^2$/N. If we take a system, divide it into N subsystems, and provide each with one redundant subsystem, the original system failure probability is squared and divided by N.

Detailed design studies of atmosphere, water, and other recycling life support systems show that a 1 in 10 probability of failure can be decreased to 1 in 10,000 by providing spares, and that the mass of spares is approximately equal to the original mass. (Jones, 2008) The above general calculation supports this. Suppose the original system probability of failure is F single = 0.1 and that the number of components is N = 100. Then F dual = $(0.1)^2$/100, or 1 in 10,000.

The approach of providing dual on-line redundancy has two disadvantages. Since both units are always operating, the failure rate and required number of repairs are both doubled. For life support systems, it is much more appropriate to provide spares that can be installed after a component failure, since the crew is available and some system repair time can be tolerated.

Analysis shows that taking a system, dividing it into N series subsystems all with equal mass and failure rates, and then providing M copies of each subsystem reduces an initial failure probability of F to [F M]/[M! N M-1]. For N = 100 and M = 2, F single = 0.1 is decreased to about F two spares = 0.5 * 10^{-4}, better by a factor of two than online redundancy. In the design of actual systems, the failure causes tend to be localized in small replaceable components, so the required mass increase to achieve high reliability is less than in this analytical formula, which is based on N subsystems all having equal mass and equal failure rates. (Jones, 2008)

Providing one spare for all the components would double the launch cost but would less than double the development cost. If there are many prototype and test units, as assumed above, the cost of providing one set of spares would be relatively small. If the quantity of full systems is increased from ten to eleven, ten percent, to allow for a full set of in flight spares, the development cost increases only six percent. The launch cost doubles. From Table 4, the total increase in the life cycle cost is 0.06 * 0.75 + 2 * 0.10 = 0.095, less than ten percent.

A. Common cause failures

Common cause failures can reduce the reliability achieved by using off-line spare parts. If a component has failure probability of 0.01 over the mission, the probability that two redundant components both fail is 0.01 * 0.01 = 0.0001, assuming no common cause failures. Typically common cause failures account for about ten percent of all the failures, so ninety percent of failures are random and independent, as usually assumed. If a subsystem has a stand-alone failure probability of 0.01 per year and a common cause failure probability of 0.001 per year, the probability that two subsystems both fail is 0.01 * 0.01 + 0.001 = 0.0001 + 0.001 = 0.0011 per year, adding the redundant pair and common cause failure rates. Redundant systems reduce the failure rate, but less than hoped for if common cause failures occur. Common cause failures can be reduced by good design, but the strongest defense is to use two diverse system designs as primary and back-up to perform the same function. (Jones, 2012, Common cause)

IX. The cost of improving reliability using diverse systems

Suppose we can develop a system for a certain life cycle cost, C, with failure probability, F, over the mission duration. If we build and operate two technically diverse systems, the total cost is 2 C and the probability that both fail is F^2. For three similar systems, the cost is 3 C and the probability that all three fail is F^3. We get much better reliability for two or three times the total cost.

The cost of developing two completely different systems to perform the same function with the same failure rate is roughly twice the cost of developing one system. Nearly all elements of the life cycle cost are duplicated, except developing the functional specification and the operations cost, since one will be off-line until and unless the other fails.

Suppose we use two identical full systems for redundancy. They can be expected to have a common cause failure rate of 0.1 F. The total failure rate for identical dual redundant systems is $F^2 + 0.1$ F. If this is nearly low enough, we could instead use component spares and get an even lower total failure rate of $F^2/N + 0.1$ F. But redundancy cannot reduce the total failure rate below the common cause failure rate.

A. Provide spares or use diverse redundant systems?

Providing spares is best if the resultine failure rate including common cause failures is sufficiently low. Spares cost much less than diverse full systems and have an additional 1/N reduction in failure rate. Diverse redundant systems are needed if the common cause failure rate is unacceptably high.

X. The cost of improving intrinsic system reliability

What is the cost of improving the intrinsic reliability of life support technology? The intrinsic reliability is defined as the probability that a single string system with no spare components will operate without failing over the mission duration. Improving intrinsic reliability can be very costly and time consuming. Developing intrinsically more reliable systems requires incurring costs for analysis, design, parts selection, process improvements, testing, failure monitoring, and redesign. There are several ways to estimate the cost to improve intrinsic reliability.

A reasonable estimate of the cost of reliability should have several properties. The cost of increasing reliability should always be greater than zero. The cost of a particular increase in reliability should be the same whether it is accomplished in one or several steps. The cost to increase reliability by a certain amount should be greater at a higher reliability. The cost of reliability equal to one should be infinite. (Aggarwall) The rules examined below meet these requirements but assume different rates of cost increase.

A. Rechtin's rule on the cost to increase reliability

Rechtin's rule of thumb in reliability design is that cutting the probability of failure in half requires an investment equal to the original development cost. If the original cost is Co for an original failure rate, Fo, of say 1 percent, it costs a second equal amount Co to achieve Fo/2 = 0.5 percent and a third amount Co to go from Fo/2 = 0.5 percent to Fo/4 = 0.25 percent. (Rechtin, p. 165) The mathematical equation for the total cost C of a failure probability F is: Rechtin cost rule = $C(F) = Co\ [1 + \log_2 (Fo/F)]$

The cost increases as the logarithm to the base two of the ratio of failure probability improvement. The cost of improved reliability according to Rechtin's rule is shown in Table 5, with other reliability cost estimating functions.

Table 5. The cost of improved reliability

Failure probability, F	Rechtin cost $C(F) = 1+\log_2 (1/F)$	Inverse cost $C(F) = 1/F$	Exponential cost $C(F) = \exp[(1–F)/F]$
1	1	1	1.00
0.5	2	2	2.72
0.25	3	4	20.09
0.125	4	8	1,096.63
0.0625	5	16	3,269,017.37
0.03125	6	32	
0.015625	7	64	
0.0078125	8	128	

Co and Fo are both set equal to one. The original cost Co = 1. The Rechtin cost increments are equal to 1. The total cost increases as 1, 2, 3, 4, etc. The failure rates are 1, ½, ¼, 1/8. A failure probability improvement ratio of eight requires a total of four times the original cost.

B. Increase intrinsic reliability, provide spares, or use diverse redundant systems?

This rule was intended to illustrate the high cost of achieving ultra reliability in space systems, but it gives a much lower cost than the exponential formula found in the reliability literature, discussed below. Even so, it can be used to show that the development cost increase to decrease the intrinsic failure probability is much larger than the mass increase to decrease failure rate by providing spares. We know that a failure rate can be decreased from Fo to $Fo^2/2$ N by providing spares that double the mass. For Fo = 0.1 and N = 50, the failure probability F is decreased to Fo * 10^{-3}. Providing 100% spares would increase the life cycle cost by less than 10 percent. Even providing diverse redundant full systems would only double the life cycle cost of a single system. In contrast, Rechtin's rule indicates that the failure rate can be decreased from Fo to Fo * 10^{-3} at a cost of eleven times the original development cost. Clearly, either providing spares or diverse redundant systems is much less costly than increasing the intrinsic hardware reliability.

C. Inverse cost rule for design to increase reliability

Rechtin says "if the original development cost X and resulted in a failure rate of 4%, then to reach 2% would require another X, to reach 1% still another X, etc." The additional costs are clearly X, X, X, etc., giving total costs of X, X + X = 2 X, 2 X + X =3 X, etc. The total cost increases as 1, 2, 3, 4 as shown above.

Suppose instead that the cost increases also increase, so that the added cost to cut the probability of failure in half is not just equal to the initial development cost, but is equal to the total of all the past cost investments. The total costs are 1, 2, 4, 8, etc. The mathematical equation for the total cost C to achieve a failure probability F is

Inverse cost rule = C(F) = Co * Fo/F

As before, Co and Fo are both set equal to one. C(F) = 1/F. This is called the inverse cost rule. The cost of improved reliability according to the inverse rule is also shown in Table 5. The total cost are 1, 2, 4, 8 for failure rates 1, ½, ¼, 1/8, since F = 1/C.

This rule can be justified as reflecting longer test time required to detect failures as the failure rate decreases. As above, suppose the failure probability is reduced by half in successive steps. Suppose equipment has an original failure rate of 1 per 200 days. Testing would produce the first failure at about 100 days. Suppose the first failure cause is corrected and the resulting failure rate is now cut in half, 1 per 400 days. Then the next failure would occur at about 200 days later. This second failure is corrected and the new failure rate is half, one per 800 days. The third failure would occur at 400 days. This failure is corrected and the new failure rate is again half, one per 1,600 days. The fourth failure would occur at 800 days. The successive test times to produce a failure are 100, 200, 400, and 800 days. If the costs to cut the failure rate increase at the same rate as the test time to demonstrate the failure rate, they increase 1, 2, 4, 8. The total cost doubles if the failure rate is halved, as per the inverse rule on cost of reliability. Rechtin's rule suggests the added costs remain equal for each successive halving of the failure rate.

D. The exponential cost of reliability function

The most used function for the cost of reliability is exponential. (Aggarwall, p. 276) (ReliaSoft)

Exponential cost rule = C(F) = a exp (b/F)

For C(Fo) = Co = a exp (b/Fo), b = Fo and a = Co/exp (1)

Exponential cost rule = C(F) = Co exp (Fo/F)/exp (1) = Co exp [(Fo – F)/F]

Co and Fo are both set equal to one. C(F) = exp [(1 – F)/F]. The cost of improved reliability according to the exponential rule is also shown in Table 5. C(1) = exp [(1 – 1)/1] = exp [0] = 1. C(1/2) = exp [(1 – 1/2)(1/2)] = exp [1] = 2.72. (exp (1) = e = 2.72. e is the base of the natural logarithms.) C (1/4) = exp [3] = 20.09. C (1/8) = exp [7] = 1,096.63. According to the exponential cost rule, the cost increases much more rapidly with F than for the Rechtin or inverse rules. See Figure 1.

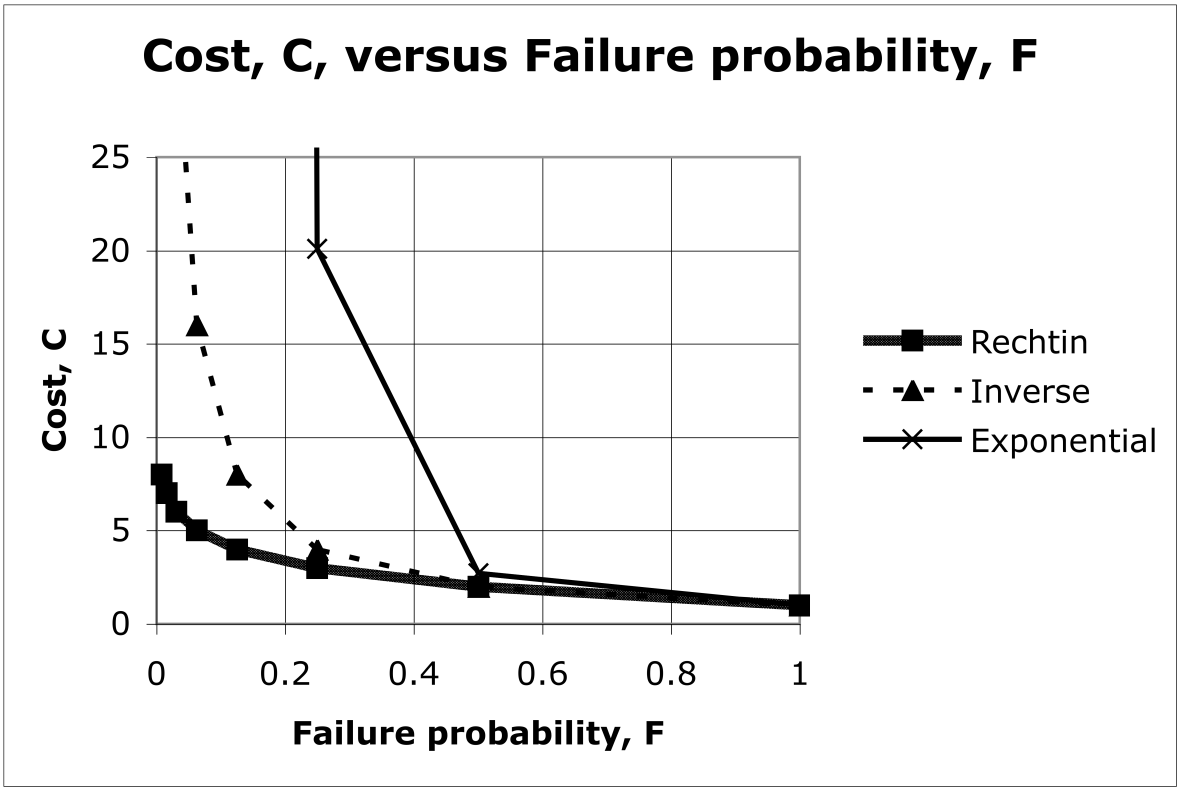

Figure 1. Cost versus failure probability for three cost rules.

For all the rules, the original cost and failure rate is 1. All the rules give the total cost to achieve failure probability F. For a failure rate of ½ of the original rate, the Rechtin and inverse rules require an additional cost of 1, and a total cost of 2. The exponential rule gives a total cost of 2.72. For a failure rate of ¼, the Rechtin rule gives a total cost of 3, the inverse rule, 4, and the exponential rule, 20. For a failure rate of 1/8, the Rechtin rule gives a total cost of 4, the inverse rule, 8, and the exponential rule, 1,097, far off the chart.

These results suggest two things. The cost to reduce failure probability by a factor of four or more could be an order of magnitude greater than the original development cost. The cost to reduce failure probability by a factor of four or more is highly uncertain.

E. Increasing intrinsic reliability is too costly

The exponential rule has been used elsewhere to show that the development cost to decrease the intrinsic failure probability is much larger than the mass increase to decrease failure rate by providing fully redundant systems. It is well known that redundancy is cheaper. (Aggarwall, pp. 279 – 280) Suppose a system costing Co has the failure rate Fo. Providing one fully redundant system increases total cost to 2 Co and reduces failure probability to Fo^2. Providing two redundant systems gives cost of 3 Co and reduces failure probability Fo^3, and in general M Co buys Fo^M. If the intrinsic failure probability is reduced by design, the failure probability Fo is reduced to Fo/2 at a cost of 2 or 2.7 Co, and to Fo/4 at a cost of 3, 4, or even 20 Co. If Fo is less than ¼, Fo^2 is less than Fo/4, and providing full redundant systems is more cost effective than increasing intrinsic reliability. And providing M spares for N components is much less expensive than providing M fully redundant systems, reducing the failure probability to Fo^M/M! N, assuming no common cause failures.

XI. How much reliability is cost effective?

Increasing reliability is very expensive. Providing spares increases the development cost somewhat and could double the launch mass and launch cost. Providing two technically diverse systems nearly doubles the entire life cycle cost. And either spares or redundancy are much less costly than increasing the intrinsic hardware reliability. The expected value of a mission can be estimated by considering the probability of failure. An investment in higher reliability is justified if it increases the expected value of the mission.

How much should be spent to increase reliability or to achieve ultra reliability? The cost effective amount depends on the cost of failure as well as the cost of reliability. If the only cost of failure is the loss of the investment in the hardware, substantially increasing the investment to go from reasonable to high reliability is not cost effective. It is better to build and fly another mission with similar cost and benefit. But if a failure would cause severe damage or a political impact, ultra reliability is needed regardless of cost. It may be that there is only one mission opportunity, or that a failure would cause loss of life. In general, spending for higher reliability is cost effective if the original failure rate is high, or if the benefit of success is much greater than the original investment cost, or if the damage due to failure is much greater than the original investment cost.

A. The value of a system and mission

Assume a system with a certain cost, C, and failure probability, F, over its mission. Suppose that a successful mission will have the benefit, B. The cost is always in cash but the benefit of manned space missions is in knowledge and prestige. Clearly B > C or the mission would not be approved and the system would not be built. If the mission succeeds, the value gained is B - C. But success is uncertain. The failure probability is F and the success probability is 1 – F. The expected value of the mission is B(1 – F) – C. The expected value must be positive for the mission to be carried out, and is large for large B and small F and C. For B(1 – F) – C > 0, B > C/(1-F). For F = 0.1, B > 1.11 C.

B. The value of increased reliability

How is the expected value of the mission affected by spending to decrease the failure probability? Using two diverse systems, we spend an additional equal cost, C, and reduce the failure rate to F^2. Then the expected value is $B(1 – F^2) – 2$ C. For this to be positive, $B > 2 C/(1 – F^2)$. For F = 0.1, B > 2.02 C, nearly twice as high a hurdle as before.

The gain in expected value is $[B(1 – F^2) – 2 C] - [B (1 – F) – C] = B[(1 – F^2) - (1 – F)] – C$. For F small, << 1, $F^2 \sim 0$. The gain in expected value is then ~ B F – C. Adding the diverse redundant system gains the benefit previously lost due to the chance of failure B F, but at the additional cost of C. Unless the failure rate is very large, F > ½, the gain of adding the diverse redundant system, B F, is less than the gain from the first system, B(1 – F). We would invest C to decrease the failure probability only if C < F B. For reasonably small F, we need C << B. It would perhaps be better to invest in a different mission with similar B, F, and C.

Increased reliability is cost effective if the original failure rate is high, or the benefit of success is much greater than the original investment cost. But there is another possible factor. There could be a cost impact or other damage if the mission fails.

XII. Possible damage caused by failure

If the mission fails, we have lost the original investment C, but that money has been spent. Suppose that damage, D, results if the mission fails. The damage may be some monetary cost, but embarrassment and loss of reputation are the usual results of failure. Whereas B > C for any reasonable mission, D is unconstrained and could be much larger than B. The expected damages are F D. The expected value of a mission with damage, D, due to failure is B (1 – F) – C – F D. The expected value is larger for large B and small F, C, and D.

A. The value of increased reliability with possible damage

As before, we assume spending another cost, C, for a diverse system and reducing the failure rate to F^2. The expected value is $B(1 – F^2) – 2 C – F^2 D$. The gain in expected value is $B[(1 – F^2) - (1 – F)] – C + (F - F^2) D]$. For F small, << 1, $F^2 \sim 0$. The gain in expected value is then ~ B F – C + F D. We would invest an additional C to decrease the failure probability only if C < F (B + D). For reasonably small F, we need C << B + D.

Increased reliability is cost effective if the damage caused by failure is high, as well as if the original failure rate is high, or the benefit of success is much greater than the original investment cost. Significant damage caused by a failure justifies investing in high reliability.

The damage due to failure is key. The blame for failure is often assigned organizationally, politically. If the blame is always assigned to engineering, management may cut the budget and schedule too severely, increasing the failure probability excessively. To increase the chance of success, everyone must be responsible for failure.

The failure of life support on a long, distant human space mission would cause loss of the crew and the mission. This catastrophe would be much more significant than the hoped-for value of the mission, so life support must be ultra reliable. Accepting more risk and a high failure rate is cost-effective for robot satellites and landers, but their

failures create strong negative public reactions, so there is a tendency to reduce scope and risk and to increase cost to improve reliability.

XIII. Approach and estimated cost and results

Achieving ultra reliability will require all three above approaches; better intrinsic single string reliability, design for the effective use of identical spares, and the use of two or more technically diverse systems to reduce common cause failures. The reliability design approach should include intensive development of at least two different technologies for each life support function.

Suppose there are two similar technologies that can be used, each with life cycle cost, C, failure probability, F, and common cause failure probability 0.1 F over the mission duration. The first step is to test and redesign the technologies to increase intrinsic reliability. We assume that doubling the development cost will cut the failure probability in half. Developing two different technologies instead of one will very nearly double the life cycle cost. Providing a full set of spares for each technology will increase the cost by about ten percent. The development cost is about three quarters of the total life cycle cost, so the overall cost for two more reliable technologies is very roughly (C + 0.75 C) * 2 * 1.1 = 3.85 C, say about four times the original life cycle cost for only one technology. See Table 6 for a detailed computation.

Table 6. Estimated cost for ultra reliability

Cost factor	Amount
Life cycle cost for one design	1.000 C
Add another development cost for higher intrinsic reliability	0.750 C
Add 10 percent of development cost to develop spares	0.1 * 0.75 C = 0.075 C
Add 10 percent of life cycle cost to launch spares	0.100 C
Subtotal - life cycle cost for one reliable design with spares	1.925 C
Double subtotal for two designs and ultra reliability	3.850 C

Since increasing the intrinsic reliability nearly doubles the cost and developing two diverse technologies again doubles the cost, while spares add little cost, a factor of four cost increase is reasonable to achieve ultra reliability. If the original life cycle cost for the entire life support system was $1.5 billion as estimated above, the new total life cycle cost for ultra reliable life support would be $6 billion.

The investment in improving intrinsic reliability of each technology cuts the single string failure probability to F/2 = 0.5 F and the common cause failure probability to 0.1 F/2 = 0.05 F. The use of subsystem spares for each technology should reduce the failure rate to $(0.5\ F)^2 + 0.05\ F$, including common cause failures, or a total of 0.3 F. The two diverse technologies have an overall failure probability of $(0.3\ F)^2 = 0.09\ F^2$. If F = 0.1, the two diverse technologies have a failure probability of 0.0009, less than one in a thousand.

XIV. Conclusion

Ultra reliable recycling life support is needed for long, distant human missions. Recycling is required on long missions to reduce the cost of life support materials. Ultra reliability is needed on distant missions since if a failure occurs, the crew cannot quickly obtain materials and spare parts or return home. Current recycling life support systems do not have ultra reliability. Achieving ultra reliability is worth its high cost because the penalty for failure on human missions is very high.

The Mars design example shows that there is less need to reduce mass and more opportunity to increase reliability than previously thought in life support research. Advanced propulsion greatly reduces the launch and emplacement cost per kilogram, so extreme efforts to reduce mass are not justified. And with lower launch cost, using spares and diverse redundancy to increase reliability is more affordable.

Achieving ultra reliable recycling life support for long, distant missions will be extremely difficult and will require a long, expensive, and sophisticated development program. The NASA mission planning community has long been aware of the need for ultra reliable life support, but incorrectly expects to see it demonstrated soon and with little further development. The NASA life support community, for various reasons, has until recently systematically neglected reliability. Careful planning and the highest priority are urgently needed now, to guide a substantial, near term, reliability focused, design and development effort.

This paper and the published Mars mission that it is based on assume that recycling life support systems will be used on a human mission to Mars. Further work done after this paper shows that directly providing all the oxygen and water may be more reliable and less costly than recycling. (Jones, 2012, Design and Analysis)

Achieving ultra reliable recycling life support requires that the systems be designed with a plan to achieve ultra reliability. The three methods to increase overall reliability are increasing intrinsic single string reliability, providing identical subsystem spares, and providing several technically diverse systems for the same functions. If ultra reliability requires providing two technically diverse systems for each function, the life cycle cost must double. Providing identical subsystem spares for a single design would have an order of magnitude lower cost, but may not achieve ultra reliability because of common cause failures. Good intrinsic single string reliability is needed for either diversity or spares to achieve ultra reliability, but achieving ultra reliability only by increasing intrinsic reliability would be orders of magnitude more costly. Increased intrinsic reliability, identical spares, and diverse systems will all be needed to achieve ultra reliability. The life cycle cost might increase four times and the failure probability could be reduced by 100.

Ultra reliability cannot be expected during mission operations, regardless of analysis and estimation, unless it has been demonstrated by the long duration test of several final systems. And it is inevitable that actual tests will discover failure modes that require redesign and retest. A short, partial retest after a redesign may fail to catch newly created flaws or adverse interactions. Achieving ultra reliability requires a long term intense reliability effort beginning many years before system operation.

References

Aggarwall, K. K., Reliability Engineering, Springer, 1993.

AMCM Advanced Missions Cost Model, JSC, http://cost.jsc.nasa.gov/AMCM.html

Carrasquillo, R. L., Carter, D. L., Holder, Jr., D. W., McGriff, C. F., and Ogle, K. Y., Space Station Freedom Environmental Control and Life Support System Regenerative Subsystem Selection, NASA TM-4340, February, 1992.

Condon, G., Tigges, M., and Cruz, M. I., "Entry, Descent, landing, and Ascent," in W. K. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Connolly, J. F., "Mars Design Example," in W. K. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

de Selding, P. B., "NASA chief: moon base first, then Mars," MSNBC, Sept. 30, 2008. http://www.msnbc.msn.com/id/26963346/

Doll, S., and Eckart, P., "Environmental Control and Life Support Systems (ECLSS)," in W. K. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Guerra, L., and Shishko, R., "Estimating the Cost of Crewed Space Systems," in W. J. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Heydorn, R. P., and Railsback, J. W., "Safety of Crewed Spaceflight," in W. K. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Humble, R. W., "Propulsion Systems," in W. K. Larson, and L. K. Pranke, eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Jones, H., "Equivalent Mass versus Life Cycle Cost for Life Support Technology Selection," SAE 2003-01-2635, 33rd International Conference on Environmental Systems, 2003.

Jones, H., "Breakeven mission durations for physicochemical recycling to replace direct supply life support," SAE 2007-01-3221, 37th International Conference on Environmental Systems, 2007.

Jones, H., "Common cause failures and ultra reliability," 42nd International Conference on Environmental Systems, 2012 (submitted for publication).

Jones, H., "Design and Analysis of a Flexible, Reliable Deep Space Life Support System," 42nd International Conference on Environmental Systems, 2012 (submitted for publication).

Jones, H., "Life Support Dependability for Distant Space Missions," AIAA-2010-6287, 40th International Conference on Environmental Systems), 2010.

Jones, H., "Multiple Metrics for Advanced Life Support" 29th International Conference on Environmental Systems, SAE 1999-01-2079, 1999.

Jones, H., "The Reliability-Mass Trade-Off in Multi-Criteria Life Support Technology Selection," AIAA-2011-5094, 41st International Conference on Environmental Systems, 2011.

Jones, H., "Ultra Reliable Space Life Support Systems," SAE 2008-01-2160, 38th ICES (International Conference on Environmental Systems), 2008.

Jones, H., and Ewert, M., "Ultra Reliable Closed Loop Life Support for Long Space Missions," AIAA-2010-6286, 40th International Conference on Environmental Systems, 2010.

Jones, H., and Kliss, M., "Air and Water System (AWS) Design and Technology Selection for the Vision for Space Exploration," SAE 2005-01-2810, 33rd International Conference on Environmental Systems, 2003.

Larson, W. K., and Pranke, L. K., eds., Human Spaceflight: Mission Analysis and Design, McGraw-Hill, New York, 1999.

Likens, W. C., "A Preliminary Investigation of Life Support Processor Reliabilities," International Conference on Life Support and Biospherics, Huntsville, AL, Feb. 18-20, 1992.

Malik, T., "Air Apparent: New Oxygen Systems for the ISS," 15 February 2006. http://www.space.com/businesstechnology/060215_techwed_iss_oxygen.html

MOCM Mission Operations Cost Model, JSC, http://cost.jsc.nasa.gov/MOCM.html

National Research Council (NRC), Advanced Technology for Human Support in Space, National Research Academy Press, Washington, D.C. 1997.

Pielke, Jr,, R., and Byerly, R., "Shuttle programme lifetime cost," Nature, 472, p. 38, 07 April 2011.

Ramamurthy, B., Franzini, B., Horowitz, E., Verges, A., Putney, B.F., and Fragola J.R., Lunar Surface Systems Risk Modeling Support Scenario 12.0.1 Element Risk Data Report, VPA/1.1/0909, NASA TASK# NNA08BA18T, Valador, Inc., September 30, 2009.

Rechtin, E., Systems Architecting: Creating and Building Complex Systems, Prentice Hall, Englewood Cliffs, NJ, 1991.

ReliaSoft, System Analysis Reference: Reliability, Availability and Optimization, 2007, http://www.weibull.com/SystemRelWeb/improving_reliability.htm

Russell, J. F., and Klaus, D. M., "Maintenance, reliability and policies for orbital space station life support systems," Reliability Engineering and System Safety, Volume 92, Issue 6, June 2007, pp. 808-820.

Wertz, J. R., and Larson, W. J., eds., Reducing Space Mission Cost, Space Technology Series, Kluwer, Dordrecht, 1996.