

Reliability Impacts in Life Support Architecture and Technology Selection

Kevin E. Lange¹

Jacobs Technology, Houston, TX, 77058

and

Molly S. Anderson²

NASA Johnson Space Center, Houston, TX, 77058

Quantitative assessments of system reliability and equivalent system mass (ESM) were made for different life support architectures based primarily on International Space Station technologies. The analysis was applied to a one-year deep-space mission. System reliability was increased by adding redundancy and spares, which added to the ESM. Results were thus obtained allowing a comparison of the ESM for each architecture at equivalent levels of reliability. Although the analysis contains numerous simplifications and uncertainties, the results suggest that achieving necessary reliabilities for deep-space missions will add substantially to the life support ESM and could influence the optimal degree of life support closure. Approaches for reducing reliability impacts were investigated and are discussed.

Nomenclature

β	=	fraction of common-cause failures
CRA	=	Carbon Dioxide Reduction Assembly
ECLS	=	Environmental Control and Life Support
ESM	=	equivalent system mass
H ₂ O	=	water
HPP	=	Homogeneous Poisson Process
ISS	=	International Space Station
k	=	number of components required for success
λ	=	component failure rate
LOC	=	loss of crew
m	=	power-law scaling exponent
MTBF	=	mean time between failures
n	=	total number of active components
N_{CS}	=	total number of component systems
r	=	total number of components available for replacement on failures
t	=	time
O ₂	=	oxygen
OGA	=	Oxygen Generation Assembly
ORU	=	orbital replacement unit
P	=	probability
R_{CS}	=	component system reliability
R_S	=	overall system reliability
RBD	=	reliability block diagram
UPA	=	Urine Processor Assembly
WPA	=	Water Processor Assembly

¹ Life Support Analyst/Chemical Engineer, ESCG, 2224 Bay Area Blvd., Mail Code JE5EA.

² Analysis Lead, Crew and Thermal Systems Division, 2101 NASA Parkway, Mail Code EC2.

I. Introduction

The goal of life support and habitation architecture is to select the capabilities with the optimal combination of mass, size, reliability, logistics, and loop closure characteristics that will best support the given mission scenario.¹

RELIABILITY will play a critical role in the design and ultimate success of life support systems for long-duration space missions outside of Earth orbit. Nevertheless, quantitative impacts of reliability have generally not been considered in life support architecture and technology trade studies. This can be attributed in part to a lack of relevant failure rate data and comparable flight-like system designs, particularly for technologies at a low readiness level.

The current study represents a simplified initial attempt to assess reliability impacts for a limited set of life support architectures applied to a one-year deep-space mission. The architectures are based primarily on International Space Station (ISS) technologies for which projected failure rates are available at an orbital replacement unit (ORU) level. Objectives include identifying key areas for architecture optimization, as well as developing a framework for future analyses. The topic of reliability impacts in life support architecture design is also discussed by Jones^{2,3} and Jones and Ewert.⁴

A. Analysis Approach

The analysis approach employed in this study seeks to compare the “cost” of alternative architectures at equivalent levels of reliability by assuming repairable systems* and adding redundancy and spares in a systematic manner to achieve target reliabilities. Equivalent system mass (ESM), a measure of relative launch cost, was selected as the initial cost metric. A more comprehensive cost metric, such as life cycle cost, could also be considered.

Future life support system designs will likely be constrained by allocations of reliability and crew time in addition to mass and volume. Optimization within these constraints will involve trades between reliability, maintenance time, and ESM. The estimation of maintenance time was not included in the current study but is a natural extension of the reliability analysis. Because reliability allocations have not been determined for future missions, a range of reliability was considered that is assumed to cover potential future requirements.

B. Definitions

For this study, the system reliability, R_S , is defined in terms of the probability of loss of crew, $P(\text{LOC})$:

$$R_S = 1 - P(\text{LOC}) \quad (1)$$

The loss of crew (LOC) end state was related to life support functional failures through a high-level fault tree analysis as described in the Appendix. Alternative end states, such as loss of mission, were not considered.

Equivalent system mass, ESM, is defined in terms of technology resource requirements and cost factors or equivalencies:

$$\text{ESM} = M + (V_{\text{PI}} \cdot E_{V_{\text{PI}}}) + (V_{\text{PS}} \cdot E_{V_{\text{PS}}}) + (V_{\text{U}} \cdot E_{V_{\text{U}}}) + (P_{\text{E}} \cdot E_{P_{\text{E}}}) + (C \cdot E_C) \quad (2)$$

where

M	=	total mass of life support equipment, consumables, and spares
V_{PI}	=	total pressurized volume of installed processors (in racks)
V_{PS}	=	total pressurized volume of stored consumables and spares
V_{U}	=	total unpressurized volume of equipment, consumables, and spares
P_{E}	=	total average system electrical power requirement
C	=	total average system cooling requirement
E_i	=	mass equivalencies (cost factors) associated with providing primary and secondary structure (based on volume), electrical power, and cooling (thermal control)

Note the different equivalencies for volume based on pressurized or unpressurized location and installed or stored state.

* Except for oxygen and nitrogen storage tanks, which are assumed to have “ k -out-of- n ” parallel redundancy.

C. Mission and Interface Assumptions

The current study was generally targeted at the class of deep space missions recently considered by NASA planning teams. Included in this class are missions to libration points, near-Earth asteroids, moons of Mars, and Mars orbit. A common feature of many of these missions is long transit times relative to the total mission duration.

Specific mission and interface assumptions employed in this study are listed below:

- 4 crewmembers
- 1-year mission duration
- single habitable module capable of long-duration life support
- negligible extravehicular activities
- no resupply, in-situ resource utilization, or propellant scavenging
- ISS-like food and hygiene systems
- metabolic and hygiene needs as defined in the NASA Human Integration Design Handbook⁵
- power, cooling, and primary structure mass equivalencies, as well as cabin volume and leakage estimates, based on a NASA Deep Space Habitat design⁶
- secondary structure (rack) mass equivalencies based on ISS

Racks were assumed necessary for installed processors to provide for maintainability.

D. Architectures

The architectures considered in this study represent different combinations of ISS regenerative Environmental Control and Life Support (ECLS) technologies in combination with either cryogenic oxygen storage or high-pressure oxygen storage. Cryogenic oxygen storage was based on the Space Shuttle technology. High-pressure oxygen storage was based on the planned Orion Multi-Purpose Crew Vehicle technology. The ISS regenerative ECLS technologies “traded” in the different architectures are the Water Processor Assembly (WPA), Urine Processor Assembly (UPA), Oxygen Generation Assembly (OGA), and Carbon Dioxide Reduction Assembly (CRA). The five combinations of these technologies considered are listed below in order of increasing life support closure:

1. Open H₂O/O₂ (none of the traded regenerative ECLS technologies)
2. WPA
3. WPA + UPA
4. WPA + UPA + OGA
5. WPA + UPA + OGA + CRA

Together with the two types of oxygen storage, a total of ten architectures were investigated.

Water and oxygen storage were included in each architecture along with ISS technologies[†] providing all other required life support functions. These functions include pressure control, nitrogen storage, carbon dioxide removal, trace contaminant control, major constituent analysis, fire detection and suppression, ventilation, temperature and humidity control, and condensate storage.

II. Reliability and ESM Analysis Methodology

A. Reliability Model Assumptions

A simplified reliability analysis was employed in this study to facilitate analytical (spreadsheet) solutions as apposed to requiring the solution of a very large number of separate Monte Carlo simulation problems. In this analysis, components (ORUs) are assumed to exist at any time in one of only three states: fully functional active, fully functional dormant (standby or spare), or failed. Additional important assumptions include:

- constant component (ORU) failure rates (exponential failure time distributions)
- perfect repair of failed components (failure rate of replaced component is same as original)
- negligible repair time for replaced components
- perfect switching for standby redundant units (components or subsystems)
- no dependent failures except those explicitly modeled as common-cause failures of identical active components
- no dormant failures

[†] All ISS technologies considered in this study are from the United States Operating Segment.

The assumption of constant failure rate implies random failures; thus spares intended for scheduled replacement of expendables and limited-life items were not included in the reliability analysis although they were included in the ESM analysis.

These assumptions were deemed acceptable for an initial analysis given the uncertainty in component failure rates and failure time distributions. It should be recognized, however, that the analysis may not capture important failure characteristics, particularly with regard to failure dependencies and consequences of different failure modes. For example, the analysis may underestimate the impacts of failure modes related to environmental influences (vibration, radiation, reduced gravity, high-oxygen atmosphere, contaminants, etc.) that could affect each replacement component in like manner. On the other hand, the analysis will overestimate the impacts of failure modes that allow repair without replacement or that do not result in complete loss of subsystem function.

B. Reliability Model Equations

For the architectures considered in this study, the system reliability can be effectively represented using a reliability block diagram (RBD) with a series structure in which each block represents a critical “component system.” A component system refers to one or more identical active base units (generally ORUs for ISS technologies) along with all standby redundant units and spares of the same type. This simple RBD structure is possible because the architectures do not contain dissimilar redundancy and because all components (except for oxygen and nitrogen tanks) are assumed to be replaceable. The latter assumption allows any redundancy at the subsystem or technology level to be equivalently represented by redundancy at the component level. With this RBD structure, failure of any component system fails the overall life support system and results in LOC. The overall system reliability is equal to the product of the component-system reliabilities:

$$R_S(t) = \prod_{i=1}^{N_{CS}} R_{CS,i}(t) \quad (3)$$

A total of 90 component systems were included in the ORU-level reliability analysis for the most complex (WPA+UPA+OGA+CRA) architecture.

The system-level RBD is illustrated in Fig. 1a. In this study, different subsystems or technologies are represented by one or more component-system blocks. In general, overlap can occur if different technologies employ common components with pooled spares.

At the component-system level, the reliability is evaluated using two approaches depending on the type of component. For oxygen and nitrogen tanks, all components (tanks) are assumed to be active and the reliability of the component system is based on k -out-of- n active parallel redundancy (k tanks are required for success out of a total of n tanks). The possibility of a common-cause failure of all tanks is included using a β -factor model. The resulting reliability expression (with the earlier assumptions) is given in Eq. (4):

$$R_{CS}(t) = e^{-\beta\lambda t} \sum_{i=k}^n \frac{n!}{i!(n-i)!} [e^{-(1-\beta)\lambda t}]^i [1 - e^{-(1-\beta)\lambda t}]^{n-i} \quad (4)$$

where λ is the component failure rate and β is the fraction of failures that result from common causes.[‡]

An RBD representation of this component-system model is shown in Fig. 1b for $k = 4$ and $n = 5$. The block labeled “C” represents common-cause failure modes.

For all other components, active components are assumed to be replaced with standby redundant components or spares upon failure. With the earlier assumptions, this replacement follows a counting process known as a Homogeneous Poisson Process (HPP) or a superimposed HPP when more than one identical component is active and spares are pooled.⁷ The resulting reliability expression is given in Eq. (5):

$$R_{CS}(t) = \sum_{i=0}^r \frac{(n\lambda t)^i}{i!} e^{-n\lambda t} \quad (5)$$

[‡] A β -value of 0.04 was assumed for oxygen and nitrogen tanks in the current analysis.

where λ is the component failure rate, n is the number of active components, and r is the total number of components (standby redundant components and spares) available for unscheduled replacement on failures. For cases where active components have different duty cycles, the failure rate based on the average duty cycle (fraction of time in operation) is used in Eq. (5).

An RBD representation of a component system with one active component ($n = 1$), one-level of standby redundancy, and two spares ($r = 1 + 2 = 3$) is shown in Fig. 1c. The switch “S” is assumed not to fail.

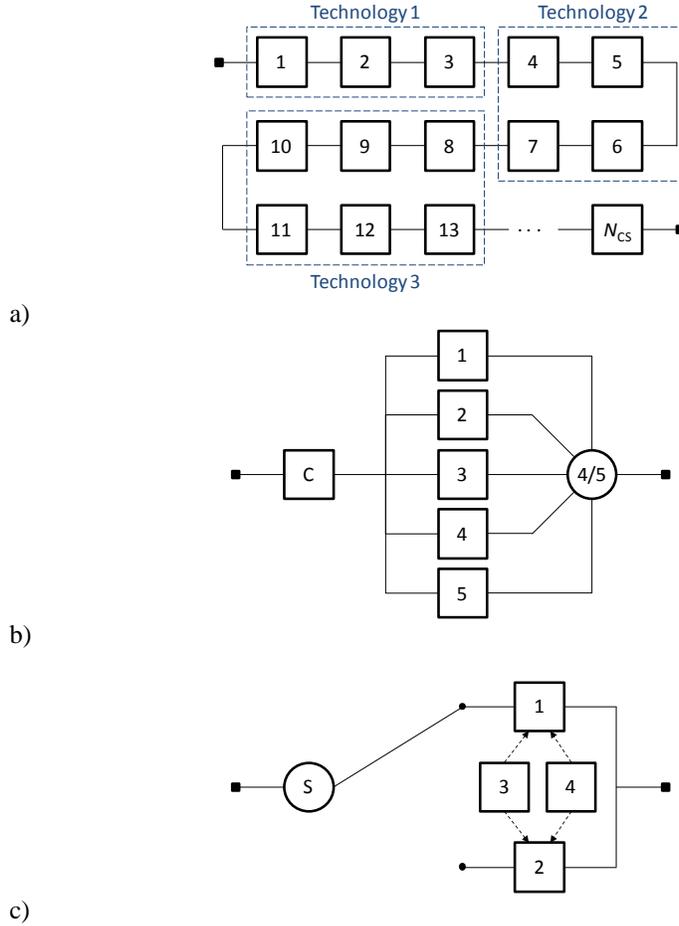


Figure 1. Reliability block diagrams: a) overall system (each block represents a component system); b) component system with 4-out-of-5 active parallel redundancy and common-cause failure mode; c) component system with standby redundancy and 2 spares.

Except for oxygen and nitrogen tanks, common-cause failure effects were not included in the initial architecture study. For a side study of divided functionality discussed later in this paper, common-cause failures of identical active (replaceable) components were included using a β -factor model. The resulting reliability expression is given in Eq. (6):

$$R_{CS}(t) = \sum_{j=0}^{\text{int}(r/n)} \left\{ \frac{(\beta\lambda t)^j}{j!} e^{-\beta\lambda t} \sum_{i=0}^{r-jn} \frac{[n(1-\beta)\lambda t]^i}{i!} e^{-n(1-\beta)\lambda t} \right\} \quad (6)$$

This equation is an extension of Eq. (5) and sums the probabilities of all success states associated with different combinations of common-cause and independent failures.[§]

[§] The integer function, $\text{int}(x)$, truncates $x = r/n$ to the nearest integer.

C. Reliability Data

Failure rates were determined from reported or estimated values of the mean time between failures (MTBF) and duty cycle using the following equation:

$$\lambda = \frac{\text{Duty Cycle}}{\text{MTBF}} \quad (7)$$

Most MTBF values for ISS ORUs were obtained from a NASA reliability and maintainability database. For ECLS technologies, these values are largely predicted (and thus considered to have high uncertainty) although some have been updated based on in-flight operational data. Where data did not exist, estimates were made based on values for functionally similar ORUs.** Failure rate estimates for oxygen and nitrogen tanks were derived from Space Shuttle and Orion design documents.

D. ESM Analysis

Technology sizing data used in ESM calculations (Eq. (2)) were obtained from a number of NASA database and document sources, including the paper by Williams.⁸ Oxygen and nitrogen storage tanks were scaled based on the specified number of tanks and the required gas storage determined from mass balances and contingency cabin repressurization requirements. Potable water storage in the form of bag-type ISS contingency water containers was also determined from architecture-dependent mass balances. Usage rates of expendables were scaled based on required daily mass flows. Other ISS technology components were not scaled except for components of the OGA and CRA, which appeared to be significantly oversized for the analyzed mission. These components (ORUs) were scaled based on mass flow using assumed power law relations.

Reported ESM values include contributions from packaged food, clothing, hygiene supplies, and waste management supplies in order to provide a more complete picture of the relative impacts of reliability on life support.

E. Reliability Improvement Analysis

The reliability of each architecture was improved by adding redundancy at the subsystem/technology level or spares at the component level. Except in the analysis of single-string architectures, one level of standby redundancy was initially added for ISS technologies that provide more time-critical functions. These include the Pressure Control System, Carbon Dioxide Removal Assembly, Trace Contaminant Control System, Major Constituent Analyzer, and Common Cabin Air Assembly (with condensate storage tank). An algorithm was employed that then further improved the system reliability in a step-wise manner by adding dormant component spares or active oxygen and nitrogen tanks. At each step, the algorithm added the spare or active tank that resulted in the greatest increase in R_S . The updated R_S and ESM were then logged and the process was repeated until a final reliability goal was achieved.

The result of the reliability improvement “process” was a set of discrete points for each architecture showing the dependence of ESM on R_S . An example of this dependence is shown in Fig. 2, where each data point represents a spare or tank addition. It was generally found that the discrete dependence could be approximated by a semi-logarithmic continuous relation as shown in the figure. These continuous relations are shown in the architecture comparisons that follow.

** For the ISS Carbon Dioxide Reduction Assembly (CRA), an early reported estimate of the overall failure rate was approximately partitioned to its different ORUs.

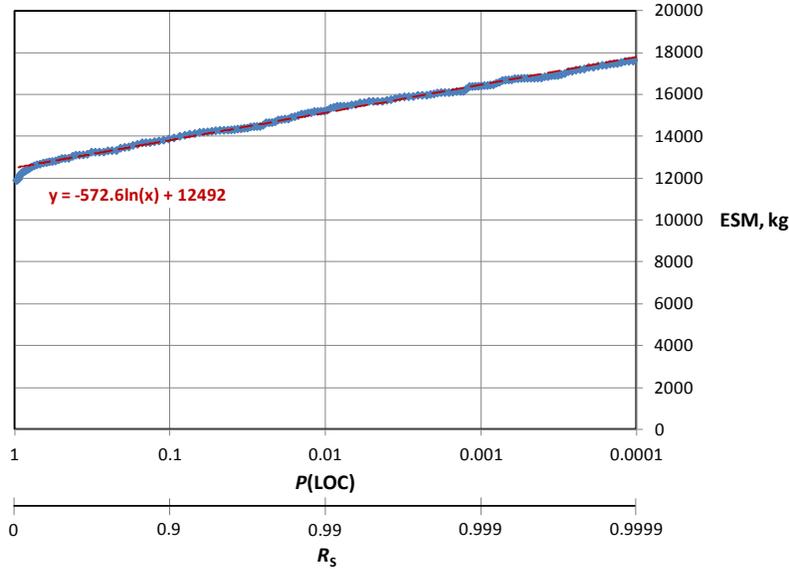


Figure 2. Growth in ESM with increasing reliability due to spare or tank addition for the WPA+UPA+OGA+CRA architecture with high-pressure oxygen storage.

III. Results and Discussion

A. Single-String Architectures without Repair

Purely single-string life support architectures have not been used on ISS or any previous manned space vehicle. Nevertheless, it serves as a useful point of reference to consider the reliability that single-string architectures would provide without unscheduled replacement spares. Table 1 compares predicted values of R_s and ESM for single-string versions of the five architectures described earlier. Results are reported for both high-pressure oxygen storage and cryogenic oxygen storage. As shown, the predicted reliabilities are very low and decrease with increasing use of regenerative technologies. The highest closure architecture (WPA+UPA+OGA+CRA) provides the lowest ESM, although by a narrow margin over architectures with more intermediate levels of closure.

Table 1. Predicted reliability and equivalent system mass of single-string life support architectures.

Architecture	High-Pressure O ₂ Storage		Cryogenic O ₂ Storage	
	R_s	ESM, kg	R_s	ESM, kg
Open H ₂ O/O ₂	0.205	15970	0.204	15310
WPA	0.056	13030	0.056	12360
WPA+UPA	0.029	11670	0.029	11010
WPA+UPA+OGA	0.011	11560	0.011	11520
WPA+UPA+OGA+CRA	0.006	10980	0.006	10940

Single-string architectures have commonly been used as a basis for comparison in previous trade studies. The implied assumption in these studies is that the results provide a valid relative ranking of technologies and architectures. The results in Table 1 and in the section that follows suggest that this approach may not be valid.

B. Multi-String Architectures with Repair

The dependence of ESM on R_s for the five architectures is shown in Fig. 3 for high-pressure oxygen storage and in Fig. 4 for cryogenic oxygen storage. These architectures include redundancy and repair as described earlier. For all architectures, the growth in ESM with increasing reliability is substantial.

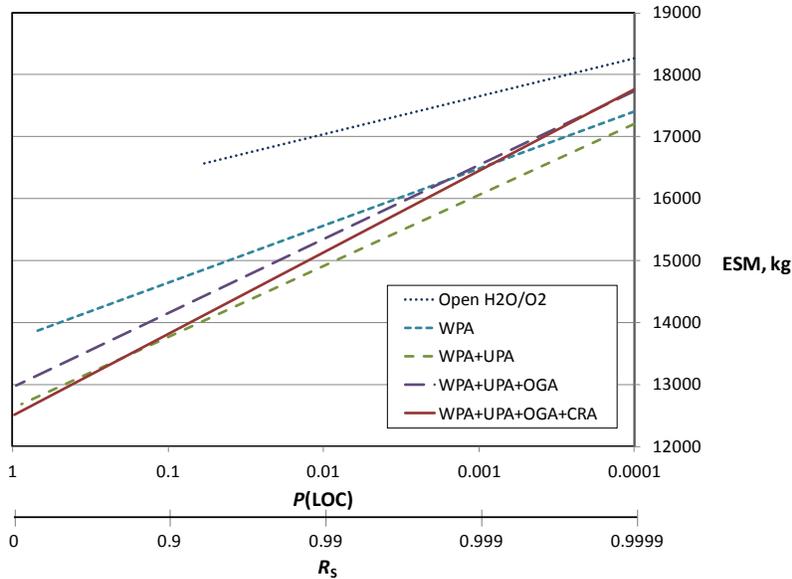


Figure 3. Reliability/ESM growth trends for different architectures with high-pressure oxygen storage.

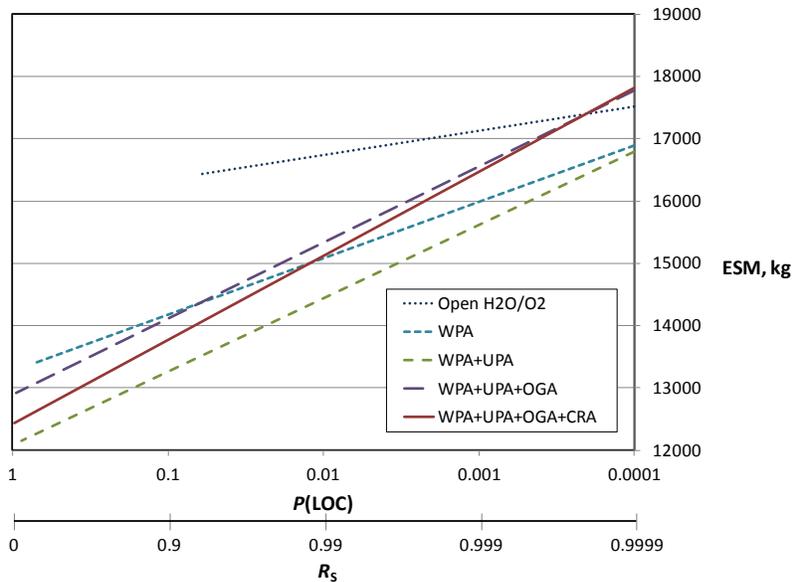


Figure 4. Reliability/ESM growth trends for different architectures with cryogenic oxygen storage.

Although reliability requirements and allocations for future missions have not been defined, it can be conjectured that a minimum acceptable overall mission reliability on the order of 0.99 ($P(\text{LOC}) \leq 0.01$) would translate into an allocated life support reliability on the order of 0.999. At this value of R_s , it can be seen from Figs. 3 and 4 that the architecture with the lowest predicted ESM is the WPA+UPA architecture. This intermediate-closure architecture recovers water from humidity condensate and urine, but uses stored oxygen. Cryogenic oxygen storage results in lower ESM than high-pressure storage and greater separation of the WPA+UPA architecture from the architectures with higher closure.

Figs. 5 and 6 explore different contributions to the ESM of each architecture at an R_s value of 0.999 with cryogenic oxygen storage. Fig. 5 compares the impact of resource type. Mass and volume ESM are seen to be the

dominant contributors for all architectures. Higher power and cooling demands with increased use of regenerative technologies do not influence the ESM ranking for the conditions of this study.

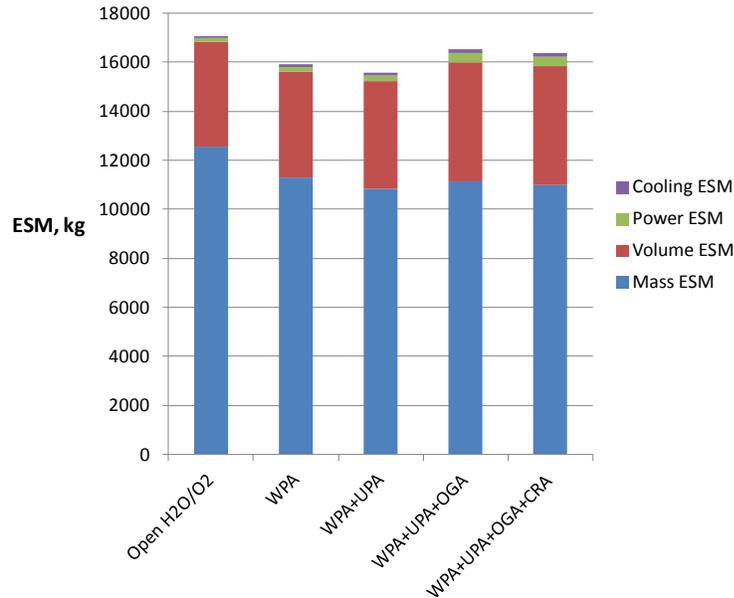


Figure 5. ESM breakdown by resource type for different architectures with cryogenic oxygen storage ($R_S = 0.999$).

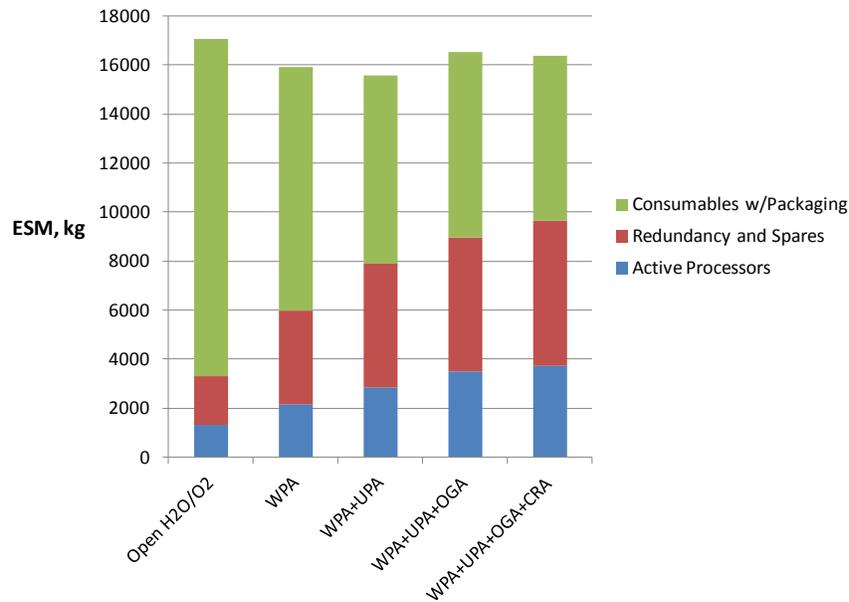


Figure 6. ESM breakdown by component type for different architectures with cryogenic oxygen storage ($R_S = 0.999$).

Fig. 6 compares the impact of component type. Consumables (with packaging) is seen to dominate for the Open H₂O/O₂ architecture and decrease in importance with increasing closure. The reduction in consumables ESM with increasing closure is offset by increases in the ESM of active processors and the ESM of redundancy and spares. For the conditions of this study, the WPA+UPA architecture provides the best ESM balance between these offsetting contributions. At this system reliability, the contribution from redundancy and spares for each architecture is greater than that of the active processors.

C. Uncertainty and Sensitivity

Considerable uncertainty exists in the component failure rates and in the effects of simplifications employed in the reliability analysis. Formal uncertainty and sensitivity analyses were not performed in this initial study, but are planned for future work. A limited global test of sensitivity was performed by repeating the analyses with all failure rates reduced by a factor of ten. Results for multi-string architectures with cryogenic oxygen storage are shown in Fig. 7. This figure can be compared with Fig. 4. Reliability impacts are still shown to be significant and the WPA+UPA architecture still has the lowest ESM for the assumed mission scenario. With high-pressure oxygen storage (results not shown), the WPA+UPA and WPA+UPA+OGA+CRA architectures have a comparable ESM at an R_S value of 0.999. These results do not reflect technology-specific uncertainties and sensitivities that will impact the degree of confidence in the architecture ESM ranking.

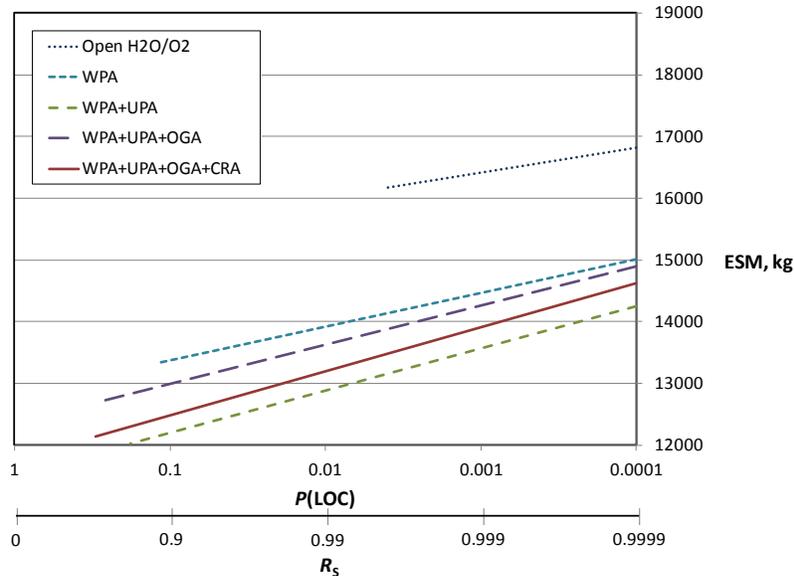


Figure 7. Reliability/ESM growth trends for different architectures with cryogenic oxygen storage. All failure rates reduced by a factor of 10.

D. Approaches to Optimization

The life support architectures considered in this study were not optimized for the assumed deep-space mission scenario. Approaches are possible at the component, technology, and architecture levels that could substantially reduce the ESM (and other cost metrics) associated with life support systems meeting reliability and crew time constraints. They include:

- Rescaling existing technologies based on new mission requirements and power/cooling resource profiles (includes reevaluating design loads and duty cycles).
- Simplifying technology and architecture designs to reduce the number of components.
- Improving component reliability through substitution or redesign.
- Reducing secondary structure costs through alternative accessibility (rack) concepts.
- Packaging components and spares to allow for lower-level maintenance.
- Using multiple subscale subsystems or components in parallel (divided functionality).
- Employing dissimilar redundancy (parallel paths in the system RBD).
- Providing distributed functional redundancy (safe-haven capability).
- Scavenging residual propellant oxygen or hydrogen for life support in missions that employ chemical propulsion (particularly for habitats that are predeployed unmanned).

Three of these approaches were investigated further: lower-level maintenance, divided functionality, and residual propellant scavenging.

1. Lower-Level Maintenance

Most ISS ECLS ORUs contain multiple functional components (valves, pumps, tanks, sensors, etc.) along with structure and plumbing. The ORU failure rate will generally be greater than the failure rates of the individual

functional components.^{††} Replacement of ORUs will therefore result in the replacement of working functional components and other non-failed parts. Maintenance at a lower functional-component level would allow more pooling of spares for common items such as valves, sensors and quick-disconnects, and could significantly reduce the total ESM of spares required to meet a given subsystem reliability allocation.

An estimate of the potential reduction in ESM with lower-level maintenance was obtained for the ISS WPA. Failure rate and mass estimates were available for the WPA at the functional component level and were used to calculate the growth in ESM with increasing subsystem reliability. Compared to ORU-level maintenance, maintenance at the functional component level resulted in a 46% reduction in ESM growth.

2. Divided Functionality

Under what circumstances, if any, is it beneficial to employ multiple subscale components or subsystems in parallel rather than a single full-scale component or subsystem? This “divided functionality” question was investigated in a separate side study that focused on the component level.

Depending on how a component scales and its sizing basis changes, the total installed mass and volume may increase with the number of parallel active components. An increased number of active components may also result in an increased probability of failures, including common-cause failures, but the replacement spares may be smaller. The component scaling dependency, total failure rate, and common-cause failure rate are therefore expected to be important variables in answering the above question.

An analysis was performed for a generic component system with the following assumptions:

- power-law scaling: component ESM $\propto (1/n)^m$, where n is the number of parallel active components and m is the power-law exponent
- 50% ESM penalty for installed components versus spares
- component failure rate does not change with scaling
- allocated component-system reliability (R_{CS}) of 0.99999

The use of a single power-law exponent to describe scaling of the component ESM implies that mass and volume are the dominant ESM contributors (power and cooling contributions generally scale differently). For $m = 0$, the component ESM does not change with n (e.g., a sensor), and the component provides full parallel redundancy. For $m = 1$, the component ESM is proportionally subdivided with increasing n (e.g., a tank). The component system reliability was calculated using Eq. (6). The number of active components, power-law scaling exponent, component failure rate, and fraction of failures due to common causes were all varied in the analysis.^{‡‡}

Results of the analysis are shown in Figures 8a-c for a total component failure rate of $10^{-6}/\text{hr}$ and for three percentages of common cause failures. The figures are projections of 3-dimensional plots in which the z -axis (out of the page) is the ESM relative to a single active component (ESM of the n -component parallel system (with spares) divided by the ESM of a single-component system (with spares)). Values of the relative ESM are represented by colors as defined in the figure legends. The power-law scaling exponent and the number of active parallel components are shown on the x and y axes.

In each figure, there is a substantial region in which the relative ESM is less than 1. These regions represent favorable trades from an ESM perspective. As expected, the most favorable region (relative ESM between 0.5 and 0.75) occurs at a scaling exponent near 1. With an increasing percentage of common cause failures, the favorable region shifts to fewer numbers of active components. The optimal number of active components may also be influenced by other cost factors such as procurement and testing costs.

These results have implications at both the component and subsystem level when considering potential commonality with other attached vehicles (such as a rover-like Multi-Mission Space Exploration Vehicle) that may be nominally sized for fewer crewmembers.

^{††} For a series RBD structure within the ORU, the ORU failure rate is the sum of the functional-component failure rates.

^{‡‡} The level of common-cause failures considered in this study was based on overall (generic) data from the nuclear industry.⁹

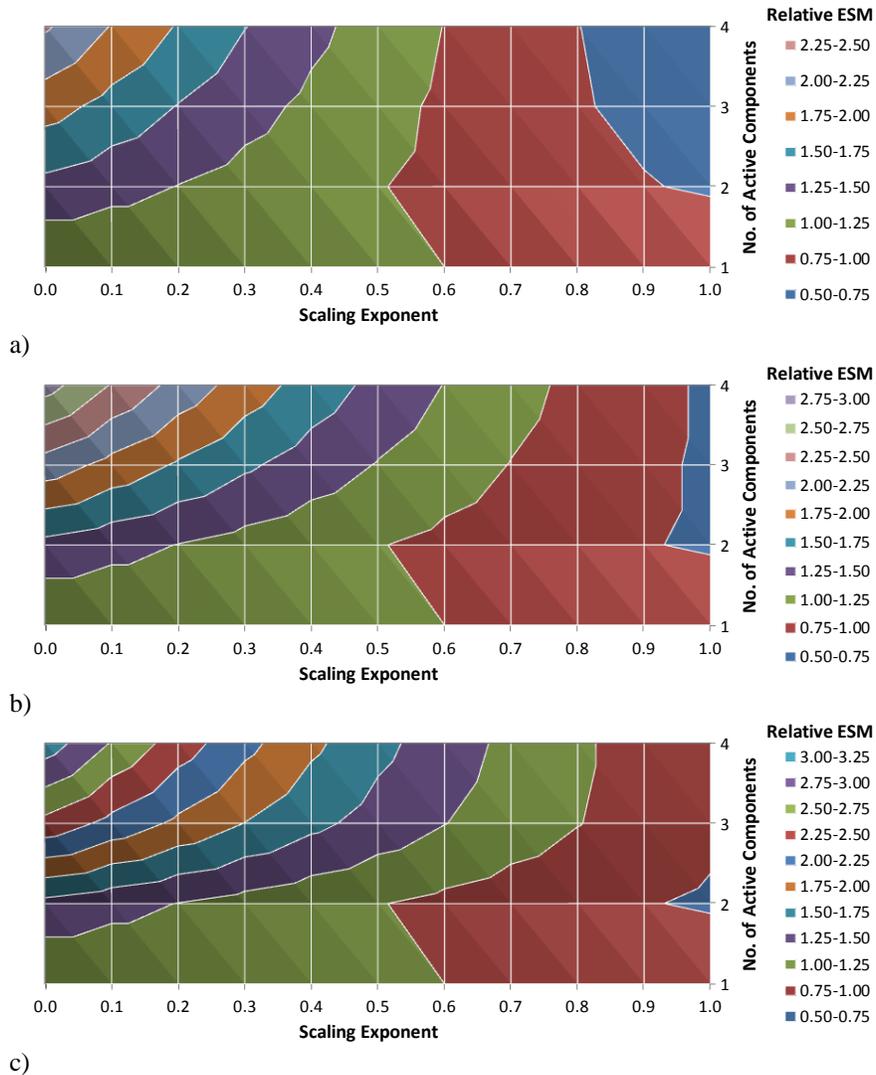


Figure 8. Impact of scaling exponent and number of active components on relative component-system ESM at three percentages of common-cause failures: a) 0%; b) 3%; c) 6% ($R_{CS} = 0.99999$, $\lambda = 10^{-6}/hr$).

3. Residual Propellant Scavenging

Some concepts for deep space missions involve prepositioning a long-duration habitat in high Earth orbit or at a Lunar Lagrange point prior to crew launch and rendezvous. Estimates of chemical propulsion requirements for such prepositioning flights suggest that the residual oxygen propellant could be comparable to or greater than the metabolic requirement of 4 crewmembers for a 1-year mission. These estimates are based on initial NASA studies and assume 3% propellant residuals. Alternative types of propulsion (e.g., solar electric propulsion) are being considered that would not provide residual propellants useful to life support.

The recovery and use of any residual propellant oxygen or hydrogen for life support would pose significant new technical challenges, but the quantities may be sufficient to warrant consideration at least for contingency (dissimilar redundancy) purposes. For prepositioned habitats, this recovery could take place autonomously before the crew launches. Residual propellant scavenging could also be considered for crewed flights.

IV. Conclusion

Although the analysis contains many uncertainties and simplifications, the results of this study suggest that reliability requirements will add substantially to the life support ESM for future missions outside of Earth orbit. Reliability impacts have the potential to negate much of the consumable savings achieved through the use of regenerative technologies. Adding additional regenerative technologies in a serial manner to the critical life support path in order to increase system closure can also effectively increase the mass of other technologies through a compensatory increase in their reliability requirements (and thus required spares).

When reliability impacts are included, all of the architectures considered in this study are likely to be unacceptable for the 1-year deep-space mission scenario. A number of optimization approaches appear possible, however, that could significantly reduce those impacts. For existing technologies, they involve a complete reassessment of design, sizing, packaging, and maintenance strategies.

Increasing system closure becomes more critical as mission duration increases. This closure involves all time-dependent consumable and replaceable quantities, including expendables and spares. A key question for life support technology developers and system architects is how to increase closure while maintaining a high-level of system reliability. At the technology level, alternatives that provide equal or greater functionality (e.g., higher water recovery) with fewer or more reliable components should be considered even if some performance metrics (such as specific power consumption) are less favorable. At the architecture level, optimal combinations of technologies in serial and parallel processing paths should be investigated. Distributed functionality and safe-haven capability should be considered in conjunction with higher-level vehicle risk assessments. Innovative solutions of the life support optimization problem are needed to provide reliable and affordable systems for future space missions.

Appendix. High-Level Fault Tree Analysis

A high-level fault tree analysis was conducted to identify critical life support functions for inclusion in the reliability and ESM analysis. Critical life support functions are those whose failure could result in loss of crew (LOC).

A fault tree relating the LOC top event to immediate causes is shown in Fig. 9. The shield-shaped “gate” below the LOC event is an “OR” gate indicating that any one of the input events below it can cause the top event. Input events shown in white can be further developed and related to loss of life support functionality and ultimately to basic events that represent failures of life support components. Grayed events are considered outside of life support.

Examples of further fault tree development to the life support functional level are shown in Figs. 10 and 11. At this level, architecture dependencies appear, such as the inclusion of oxygen generation in Fig. 10 and carbon dioxide reduction in Fig. 11. By developing the fault tree in a top-down manner from immediate causes of LOC, the life support functional requirements and functional decomposition are essentially derived. This type of analysis becomes more critical when more complex architectures involving dissimilar redundancy and multiple-module safe-haven scenarios are considered.

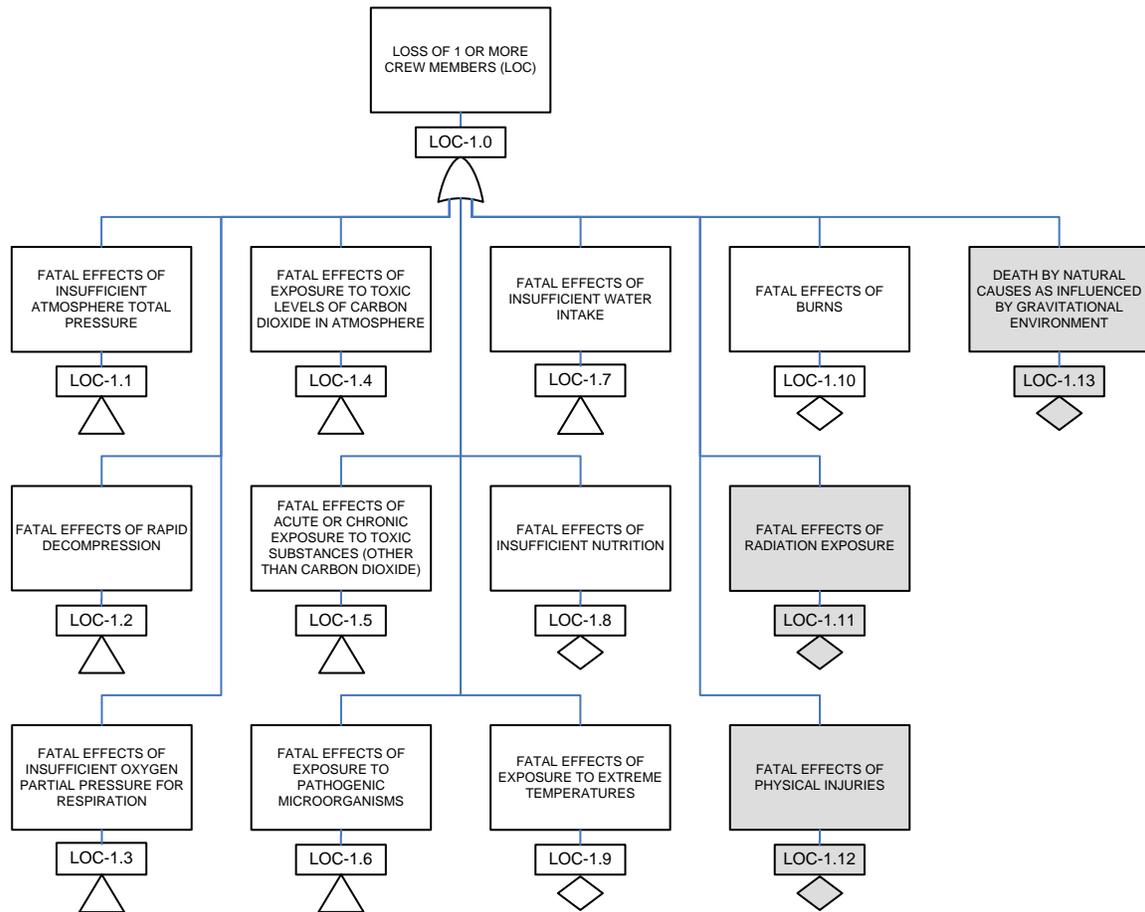


Figure 9. Top-level LOC fault tree. Grayed events are outside of life support.

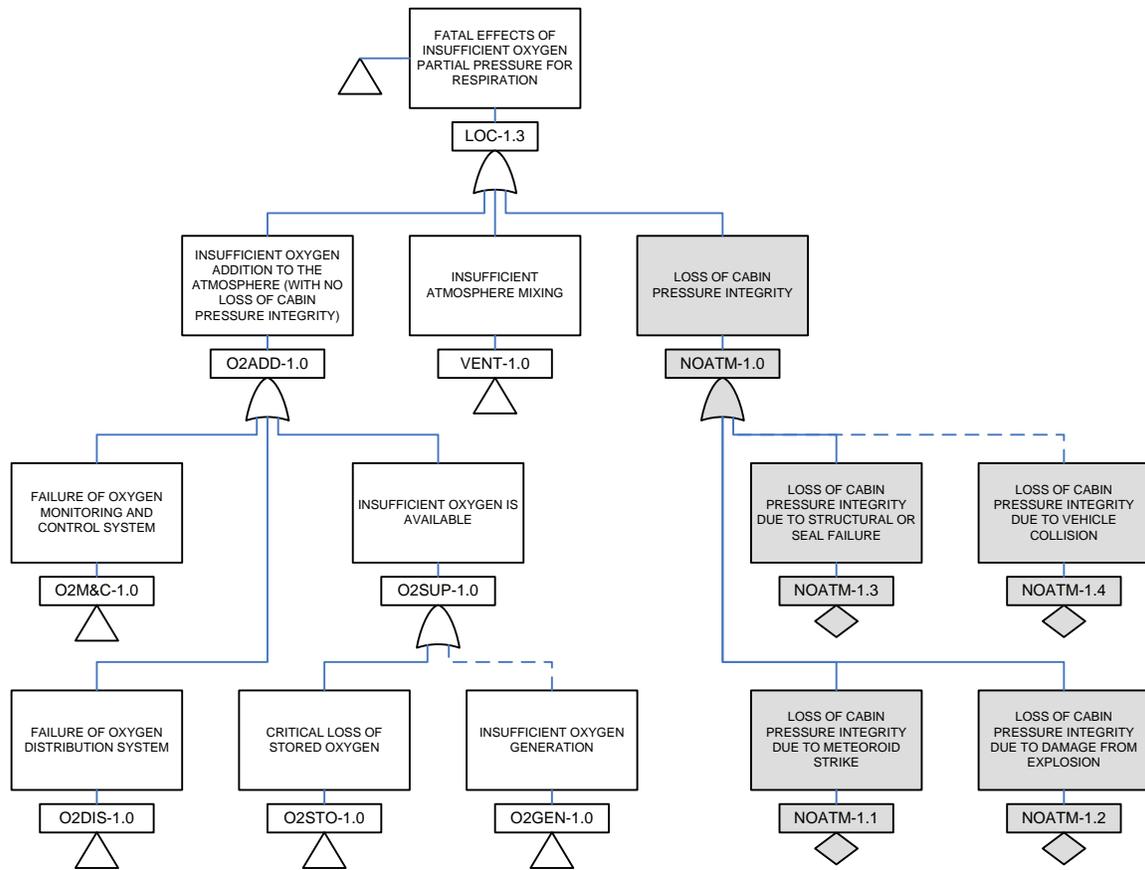


Figure 10. Further development of the event related to insufficient oxygen partial pressure for respiration (based a single long-duration habitable module). Grayed events are outside of life support. Dashed lines indicate architecture or mission dependency.

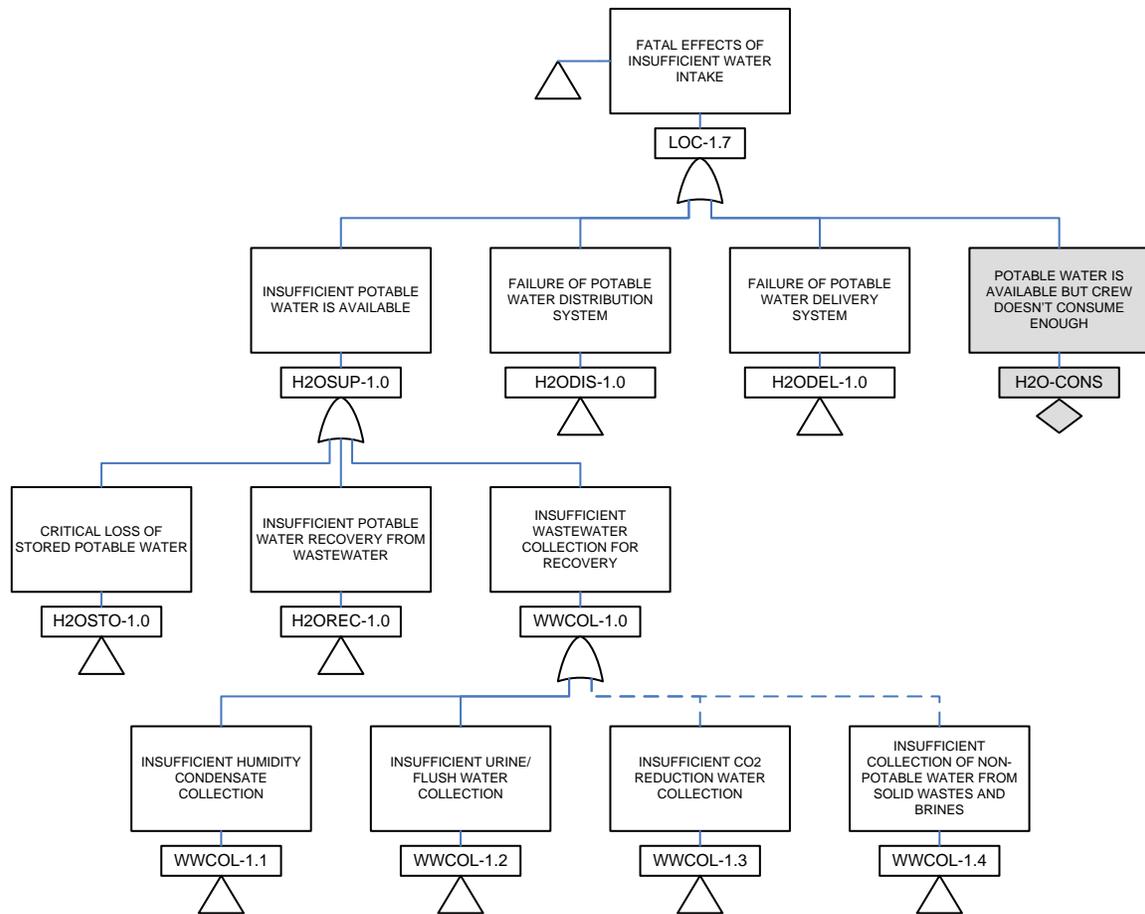


Figure 11. Further development of the event related to insufficient water intake. The grayed event is outside of life support. Dashed lines indicate architecture dependency.

Acknowledgments

The authors wish to thank Dr. Dan Barta and Mr. Mike Ewert for their support of this work.

References

- ¹Hurlbert, K., Bagdigian, B., Carroll, C., Jeevarajan, A., Kliss, M., and Singh, B., "Draft Human Health, Life Support and Habitation Systems – Technology Area 06," NASA Draft Space Technology Roadmap, November 2010, URL: <http://www.nasa.gov/offices/oct/home/roadmaps/index.html> [cited 22 March 2012].
- ²Jones, H., "Ultra Reliable Space Life Support Systems," *SAE Int. J. Aerosp.*, Vol. 1, No. 1, 2009, pp. 482-498.
- ³Jones, H., "The Reliability-Mass Trade-Off in Multi-Criteria Life Support Technology Selection," AIAA-2011-5094, 41st International Conference on Environmental Systems, July 2011.
- ⁴Jones, H., and Ewert, M., "Ultra Reliable Closed Loop Life Support for Long Space Missions," AIAA-2010-6286, 40th International Conference on Environmental Systems, July 2010.
- ⁵NASA, "Human Integration Design Handbook (HIDH)," NASA/SP-2010-3407, January 2010.
- ⁶Toups, L., Smitherman, D., Shyface, H., Simon, M., Bobskill, M., Komar, D. R., Guirgis, P., Bagdigian, B., and Spexarth, G., "Deep Space Habitat Team: HEFT Phase 2 Efforts," NASA/ESA Bilateral Meeting, January 2011, URL: http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20110006982_2011003312.pdf [cited 22 March 2012].
- ⁷Rausand, M., and Høyland, A., *System Reliability Theory – Models, Statistical Methods, and Applications*, 2nd ed., John Wiley & Sons, Hoboken, New Jersey, 2004.
- ⁸Williams, D. E., "Summary of Resources for the International Space Station Environmental Control and Life Support System for Core Complete Modules," SAE 2004-01-2386, 34th International Conference on Environmental Systems, July, 2004.
- ⁹U.S. Nuclear Regulatory Commission, "CCF Parameter Estimations, 2010 Update", January 2012, URL: <http://nrc.nrc.gov/resultsdb/ParamEstSpar/> [cited 22 March 2012].