JOURNAL OF SPACECRAFT AND ROCKETS
Vol. 48, No. 2, March–April 2011

Prediction of Reliability for Environmental Control and Life Support Systems

Haibei Jiang* and Luis F. Rodríguez†
University of Illinois at Urbana-Champaign, Urbana, Illinois 61801
Scott Bell‡ and David Kortenkamp§
NASA Johnson Space Center, Houston, Texas 77058
and
Francisco Capristan¶
Georgia Institute of Technology, Atlanta, Georgia 30332

DOI: 10.2514/1.44792

An increasing awareness of life-support system reliability has been noticed in the aerospace community as long-term space missions become realistic objectives. Literature review indicates a significant knowledge gap in the accurate evaluation of the reliability of environmental control and life-support systems. Quantitative determination of system reliability, however, is subject to large data requirements, often limiting their applicability. In an effort to address this issue, this paper presents an approach to reliability analysis for life-support system design. A simulation tool has been developed with the capability of representing complex dynamic systems with configurable failure rate functions for life-support hardware. This tool has been applied and compared with classical reliability prediction approaches. As a result of this work, it has been determined that typical life-support system configurations are likely to be more reliable than classical approaches might suggest. This is due to an inherent buffering capacity in life-support system design, which might be leveraged to improve the cost effectiveness of future life-support system design.

Nomenclature

$F(t)$	=	cumulative failure function
$f(t)$	=	probability density function
$L(X_1, \ldots, X_n; \Theta)$	=	the likelihood function of the system described by failure data $X_i, \ldots, X_n$, as controlled by the mean likelihood estimator Θ
$\min(a, b, c)$	=	minimum function, returning the smallest value of a, b, and c
n	=	the number of data points used to determine the mean likelihood estimator of the exponential distribution
$R(t)$	=	system reliability
$R_i(t)$	=	reliability of subsystem i
T_i	=	the estimated mean time to failure of subsystem i
T_{sys}	=	the estimated mean time to failure of the system
β	=	a characteristic parameter of the two-parameter Weibull distribution
Θ	=	the mean likelihood estimator
λ	=	the characteristic parameter of the exponential distribution, and a characteristic parameter of the two-parameter Weibull distribution. In the case of the exponential distribution, generally units are failure per unit time, or failure/hour, in this case. The reciprocal of lambda is generally regarded as the mean time to failure of the exponential distribution. In the Weibull distribution, λ is a shape parameter.
λ^*	=	the predicted value of the mean likelihood estimator of the exponential distribution
μ	=	one of the two characteristic parameters describing the normal distribution. Generally the units of μ are in time, hours in this case. The mean time to failure of the normal distribution is μ.
σ	=	one of the two characteristic parameters describing the normal distribution, generally σ is a unitless measure of variance

Presented as Paper 2008-7818 at the AIAA SPACE 2008 Conference & Exposition, San Diego, CA, 9–11 September 2008; received 28 April 2009; revision received 29 September 2010; accepted for publication 7 November 2010.

*Graduate Student, Department of Agricultural and Biological Engineering and Department of Aerospace Engineering, 376D Agricultural Engineering Sciences Building, MC-644, 1304 West Pennsylvania Avenue, Urbana, IL 61822.

†Assistant Professor, Department of Agricultural and Biological Engineering, 376C Agricultural Engineering Sciences Building, MC-644, 1304 West Pennsylvania Avenue, Urbana, IL 61822 (Corresponding Author). Member AIAA.

‡Research Scientist, TRACLabs Inc., 1012 Hercules.

§Senior Scientist, TRACLabs Inc., 1012 Hercules. Member AIAA.

¶Undergraduate Student, School of Aerospace Engineering, 47 Northwest Boulevard, Miami, FL 33126.

I. Introduction

LARGE-SCALE complex environmental control systems such as those considered by NASA feature nondeterministic characteristics. These systems are not accurately represented by combinations of series and parallel reliability block diagrams, thus they present major challenges for quantitative risk analysis. Nevertheless, robust environmental control and life-support systems with multidegree fault tolerance and well-proven contingency plans are desired by NASA and its space exploration program.** Long-duration human activity in a Lunar Outpost has been proposed as a gateway to future Martian exploration. As mission length increases, resupplies of food, water, air, and life essentials become more and more costly. Since crew survivability is the most important factor in manned space exploration, designing and building an authentically reliable regenerative life-support system is of critical importance.

**See Exploration Life Support Overview available at http://els.jsc.nasa.gov/ [Accessed 9 December 2009].

The classical design of reliable systems involves accurate prediction of random component failure, the related cascading effects, contingency planning, and maintenance strategies.

Current NASA reliability analysis is a "lessons learned" style database built on historical data and expert opinions. Reliability, or failure probability, is determined by experiment or, more often, by assumption. A widely used database compiled based on the International Space Station (ISS) is known as the ISS Risk Management Application (IRMA) [1], which emerges from the Futron Integrated Risk Management Application.[††] It uses a two-dimensional risk assessment approach to predict likelihood and consequence of any given event. These judgments are made by designers, operators, astronauts, and analysts in a score matrix. Possible reliability issues will thus be addressed according to the priority decided by these scores. NASA has also developed a Probabilistic Risk Assessment (PRA) tool considering the failure modes of the Space Shuttle.[‡‡] In this case, failure modes are identified by personnel working in Space Shuttle design, maintenance, operations, or analysis. Failure modes and their related effects are evaluated for their impacts on system health. Failure Modes and Effects Analysis (FMEA) [2] is a similar approach, popular in the industry due to its successful applications in many important projects, such as the Concorde and Airbus projects [3], the Lunar Module, and many other applications, such as military systems, car manufacturing, and nuclear power plants [4,5]. Other alternative approaches exist as well, including Fault Tree Analysis (FTA) [6], What-If Analysis, Functions-Components-Parameters Analysis (FCP) [7], and Hazard and Operability Method (HAZOP) [8], all coming from analogous challenges existing within the chemical processing or nuclear industry [9,10]. The limitation of these approaches can be summarized as follows:

1) All these approaches heavily rely on operational data, which can only be acquired after the systems is operational.

2) The magnitude of effort required to assemble all the possible failure modes limits their applicability.

3) In the case there is a large but incomplete amount of data available, the effectiveness of the analysis depends heavily on the focus and objectivity of the assessment team due to the inherent subjectivity of individuals close to the system.

4) None of the existing approaches can address the impact of buffering capacity, repairable components, maintenance quality, or reliability degradation.

Overall, these limitations reveal the concern that the classical reliability and risk analysis approaches may not be precise and effective for systems like life-support systems. In the case of environmental control and life-support system (ECLSS), there exists a demonstrated capacity to recover from major system failures given the ingenuity of crew and mission control and an opportunity to provide corrective maintenance. For example, recall the miraculous recovery during the Apollo 13 mission, where the very volume of the habitat provided enough of a buffer to allow the crew and mission control to reconfigure the system and return to Earth safely. It is this *buffering capacity* that we seek to quantify here by considering the design of ECLSS. Buffering capacity in life-support system design is represented by additional stored resources in the crew habitat environment or in storage buffers. These resources can be used by the crew in the event of failure of life-support hardware, and can prove critical in ensuring crew survival. Moreover, as mission length and distance from Earth increases, crew challenges such as the failure of life-support hardware must be expected and contingency plans will need to be prepared considering limited availability of support from Earth. With better quantification of the amount of buffering capacity available, contingency design can be based on a quantitative understanding as to which resources define the most critical buffers. It is shown here that the buffering capacity of ECLSS can have a large impact on the accuracy of standard reliability approaches and, therefore, alternative methods should be considered.

This paper will present the recent findings to address this challenge. The main contribution of this paper lies in the demonstration of the capability of several developmental reliability assessment approaches and a component-based simulation tool for studying the reliability and cost of complex environmental systems in space applications. The virtual environment we built is intended to deliver the following advantages:

1) Provide a virtual test bed, which allows mission designers to test different system designs and study the tradeoff between design and system reliability.

2) Predict the reliability function for the integrated system based on component reliability functions.

3) Determine the minimum component reliability requirements given various system level reliability objectives.

4) Test different corrective and preventive maintenance strategies to determine the optimal maintenance scheduling.

5) Compare system ESM (equivalent system mass) and MTTF (mean time to failure).

6) Address the buffering capacity in ECLSS and its impact on system reliability and cost.

Because of the complexity of the problem and the depth of study we plan to conduct, the overall objectives of this study can be divided into three interrelated phases.

Phase I: Compare life testing results using classical reliability block diagrams, modified reliability block diagrams, and simulation experiments coupled with quantitative statistical methods.

Phase II: Establish a reliability theory which considers system buffering capacity (similar to *response delay* defined in modern control theory). With such a theory, the objective is to obtain more accurate reliability prediction results using a modified conventional reliability theory in studying complex environmental systems.

Phase III: Model preventive and corrective maintenance functions and study the impact of their quality and schedules. Demonstrate the importance of employing appropriate contingency plans by testing systems with and without them. Optimize system design by balancing the tradeoff between reliability and cost. Reconfigurable control systems can be designed and tested at this stage as well.

The first two phases of the plan have been completed and the corresponding results are presented in this paper. The remainder of the paper is organized as follows: Sec. II introduces the reliability prediction approaches adopted for this analysis, including reliability block diagram, modified reliability block diagram, simulation experiments, and statistical methods; Sec. III describes a simplified life-support system in a 180-day Lunar Outpost mission used as a case study here. Section IV discusses the experimental results obtained for this system; Sec. V presents the conclusions and the directions for future research.

II. Methodology

Four reliability prediction methods, RBD (reliability block diagram), MRBD (modified reliability block diagram), MTTF (mean time to failure), and MC (Monte–Carlo) style simulation with MLE (maximum likelihood estimation), and the reasoning behind their selection are discussed here. Each of these four methods are contrasted in their ability to predict the reliability of an ECLSS designed for a Lunar outpost mission. Subsequently, a sensitivity analysis used to quantify the impact of the buffering capacity is introduced.

A. Reliability Modeling and Prediction Approaches

1. *Reliability Block Diagrams*

A fundamental approach to represent system reliability in terms of component reliability is the use of RBDs [11]. Component interactions are presented by a network of blocks in accordance to the actual physical relationship of the components in the system. Let n denote the number of components in the system, four special configurations are depicted in Fig. 1 where:

1) System A represents a *series system*.

[††]"Risk Management: Futron Integrated Risk Management Application (FIRMA)," http://www.futron.com/ [Accessed July 2009].

[‡‡]"Probabilistic Risk Assessment: What is it and Why is it Worth Performing," http://www.hq.nasa.gov/office/codeq/qnews/pra.pdf [Accessed August 2009].

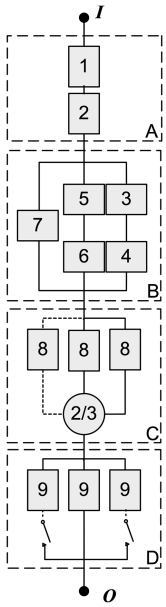

Fig. 1 Reliability block diagrams.

2) System B represents a *parallel system*.
3) System C represents a *k-out-of-n system*.
4) System D represents a *system with passive (offline) redundancy*.

In conventional reliability theory, the integrated system is in an operational state when there is an open pathway between the start I and end O, representing the inputs and outputs of the system; the system is determined to be in a failed state when there is no continuous path between I and O. The advantage of such a graphical representation of system configuration is that the reliability can be determined using a binary characterization of the state of each component within the system. A time-variant binary structure function, $\Phi(t)$, equals one if the system is in a working state (UP), and zero if the system is in a failed state (DOWN). Thus, the reliability can be defined as the probability that the structure function Φ is equal to one, $R(t) = P(\Phi(t) = 1)$. Mathematically, the reliability function of a series system can be expressed as

$$R(t) = R_1(t)R_2(t)\ldots R_n(t) = \prod_{i=1}^{n} R_i(t) \tag{1}$$

For parallel systems, the reliability function is

$$R(t) = 1 - F_1(t)F_2(t)\ldots F_n(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t)) \tag{2}$$

The generalized *k-out-of-n* system is commonly used for systems with higher reliability requirements. This type of reliability improvement is also known as active (online) redundancy. The reliability function of such systems can be mathematically represented in the form

$$R(t, n, k) = \sum_{r=k}^{n} \binom{n}{r} R(t)^r (1 - R(t))^{n-r} \tag{3}$$

Passive (offline) redundancy considers a two-unit system where a standby unit assumes the function of the primary unit. The reliability of the system is the sum of the probability that the primary unit does not fail before time T and the probability that the primary unit fails at some time $\tau, 0 < \tau < T$ while the standby unit functions successfully from τ to time T. Mathematically

$$R(T) = R_1(T) + \int_{\tau}^{T} f_1(t)R_2(T - t)\,\mathrm{d}t \tag{4}$$

where R_1 and R_2 denote the reliabilities of the primary unit and the standby unit, respectively, and f_1 is the probability density function describing the failure of the first unit. More generally, we can extend the two-unit standby system to a n-unit standby system with the assumption that each unit process has a constant failure rate λ. The reliability of such a multiunit standby system is given by

$$R(t) = e^{-\lambda t}\left[1 + \lambda t + \frac{(\lambda t)^2}{2!} + \ldots + \frac{(\lambda t)^{n-1}}{(n-1)!}\right] \tag{5}$$

In general, these reliability functions indicate that system reliability increases as the number of standby units increases. However, the rate of system reliability improvement decreases exponentially as the number of standby units increases. Maintenance and cost requirements increase with additional standby units. Hence, a decision regarding the number of standby units needed by the system needs to be made, which should account for both the cost of adding standby units and the requirements for system reliability.

To properly apply these methods to life-support system analysis, several critical assumptions need to be made. Conditional component failure probability functions are currently unknown, thus independent component failures have been assumed. It is currently assumed that no preventive or corrective maintenance is available for system components. Such contingency plans are to be tested in the future.

2. *Modified Reliability Block Diagrams*

The modified reliability block diagram approach is introduced for the purpose of modeling the buffering capacity in life-support systems. The buffering capacity exists inherently in ECLSS given that system failure is no longer defined by component states alone, rather the crew state and their productivity determines system failure. The major innovation presented here is the use of reliability blocks to represent the system buffering capacity which supports crew habitat after certain regenerative components fail. A graphical representation of the modified system reliability diagram is depicted in Fig. 2. The blocks in subsystem E represent the buffering capacity, or more generally, the remaining resources in the environment. The blocks numbered 10, 11, 12, and 13 contain the same resource that is produced by system A, B, C, and D, respectively. They will begin to provide the necessary resources to keep the crew members alive when regenerative system A, B, C, or D fail to be functional. This modification in system reliability diagram is believed to affect system reliability prediction results since the system will not fail instantly even if the components are connected in a series configuration.

To quantify the reliability of such a system appears to be straight forward since it is very similar to a parallel configuration. However, the challenge of selecting a failure function that represents the

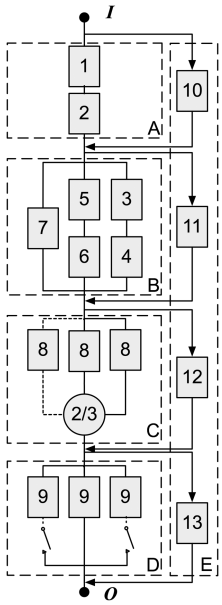

Fig. 2 Modified reliability block diagrams.

buffering capacity is not trivial. Intuitively the buffering capacity would be related to the design of the ECLSS, however, proper buffering capacity sizing is still to be addressed. At the current stage, we assume that the environmental buffers are idle when the regenerative components are functional, and they will only be activated under the circumstances when the production of a certain resource is ceased due to a component failure.

A normal reliability model has been proposed to represent the buffering capacity. The advantage of a normal model is that it can mathematically simulate binary states. It can also be used as a system reliability indicator since the probability of system failure is one when the reliability of buffer becomes zero. Physically this means that a critical resource has been exhausted and crew failure is imminent. Mathematically, a normal reliability model can be expressed in the following form:

$$R(t) = 1 - F(t) = 1 - \int_{-\infty}^{t} \frac{1}{\sigma\sqrt{2\pi}} e^{[-\frac{1}{2}(\frac{\tau-\mu}{\sigma})^2]}\, d\tau \tag{6}$$

where μ and σ are, respectively, the mean and the standard deviation of the distribution. The plot in Fig. 3 has a very sharp reliability decrement after 4320 h since the selected μ and σ are 4320 and 1, respectively. These values need to be carefully selected by the system analyst for properly sizing the buffering capacity for real systems.

3. *Mean Time to Failure Approach*

An alternative for approximating system reliability is the direct use of component MTTF. This is a deterministic method based on the reliability assumptions for individual components. For a series system, $\text{MTTF}_{\text{sys}} = \min\{\text{MTTF}_1, \text{MTTF}_2, \ldots\}$; for a system with active redundancy, $\text{MTTF}_{\text{sys}} = \max\{\text{MTTF}_1, \text{MTTF}_2, \ldots\}$; for a system with standby redundancy, $\text{MTTF}_{\text{sys}} = \sum_{i=1}^{n}\{\text{MTTF}_i\}$, where n is the number of standby components. The major advantage of this approach is its convenience.

4. *Monte–Carlo Style Simulation with Maximum Likelihood Estimation*

BioSim is a dynamic system simulation tool developed by NASA Johnson Space Center [12–14], which includes mathematical models for typical components found in various life-support systems. The BioSim tool has been used here to create a Monte–Carlo style simulation of ECLSS. These models are fully integrated and highly configurable. Simulation progresses in hourly time increments. An extensible markup language configuration file containing the design of the system initializes the simulation and defines parameters for random failure and stochastic performance [15]. BioSim has been successfully used and verified in many ECLSS design applications, including optimization [16], reliability analysis [15], control system testing [17], and power system design verification [18]. For simulation purposes, several additional assumptions should be noted:

1) For all stores, if the amount of resources to be stored exceeds their designed capacities, the extra materials will be dumped into space.

2) WRS has 100% conversion efficiency.

3) Crew daily schedule is: 8-h of sleep (intensity level of 0), 12-h of lab work (intensity level of 2), and 4-h of exercise (intensity level of 4).

4) The initial power, food, and water storage levels are designed to satisfy the nominal mission length.

Monte–Carlo Simulation [19] (MC) allows the analyst to consider a wide array of outcomes that the system may encounter. The simulation environment we developed enables us to study many reliability features which cannot be easily captured by analytical models, such as different maintenance schedules and quality, reliability degradation, repair priorities, and the focus of this paper, buffering capacity. In this study, five reliability testing experiments are conducted, each of which involves destructive simulation of 100 identical systems, whose failure times and causes are captured for reliability prediction. In our application, the major concern is that even if numerous trials have been conducted, there is no guarantee

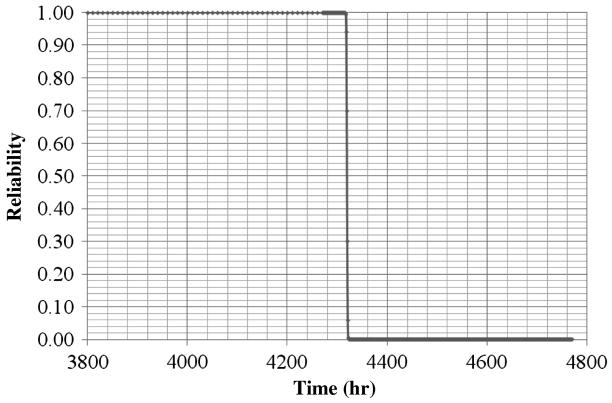

Fig. 3 A normal reliability function with $\mu = 4320, \sigma = 1$.

that we can exhaustively span the entire search space and identify all the possible malfunctions and consequences.

Maximum Likelihood Estimation (MLE) method is one of the most widely used methods for estimating the parameters of a probability distribution function using the likelihood function. The likelihood function L is given by

$$L(X_1, \ldots, X_n; \Theta) = \prod_{i=1}^{n} f(X_i; \Theta) \tag{7}$$

The maximum likelihood estimator of Θ, or Θ^*, of a probability density function will maximize L. In most cases, the maximum likelihood estimator is obtained by differentiating Eq. (7), setting equal to zero and solving for the maximum likelihood estimator. For an exponential distribution, the characteristic variable is the failure rate λ, and the maximum likelihood estimator, λ^*, is determined by taking the reciprocal of the mean of the failure [Eq. (8)]

$$\lambda^* = \frac{n}{\sum_{i=1}^{n} x_i} = \frac{1}{\bar{x}} \tag{8}$$

where x_i is the failure time of the ith component under test. MTTF is simply the inverse of λ^*.

The same approach can be applied to many other widely used reliability models, such as the two-parameter exponential distribution model, the Weibull distribution model, the normal and lognormal distribution model, and the inverse Gaussian distribution model. The final selection of system reliability model needs to be made so as to best match the actual experiment results. If any of these probability distribution functions can adequately model the failure data of the system, the parameters of those distributions can be identified using this approach.

Parameters identified can be subsequently used to predict reliability, $R(t)$. In the case of the exponential distribution, the form of the reliability function is as in Eq. (9)

$$R(t) = e^{-\lambda^* t} \tag{9}$$

B. Sensitivity Analysis

A sensitivity analysis was conducted to study the relationship between varying buffer sizes and system reliability. It was determined through this work that the crew atmospheric environment defined a key resource and therefore the analysis focused on the impact of varying the size of this buffer. Seven different environmental buffer sizes ranging from 15 to 105 days of life-support capacity were considered. The MRBD approach and MTTF approach were employed to estimate the system reliability boundaries. In the MRBD approach, 100 system failure times were captured for each buffer size and the average value was used to calculate the system reliability parameter, assuming an exponential reliability model. The MRBD approach was used to predict the lower bound for system reliability, while the atmospheric buffer was modeled in parallel to the air revitalization subsystem. The MTTF approach was

considered to be more optimistic and, therefore, it is used to predict the upper bound for system reliability.

III. Case Study: Lunar Outpost

The ECLSS considered in this study is designed for a six-month Lunar Outpost mission. It consists of four types of components: *bulk storage components* (i.e., gases and water), *regenerative components* (i.e., an oxygen generation system and a water recovery system), *control components*, and *crew members*. A typical series configuration of such a system is depicted in Fig. 4, where the mass and power flow is shown. In Fig. 4, horizontal cylinders represent regenerative processors and vertical cylinders represent storage units. Arrows represent the flow of mass from one unit to the next. Line type is used to represent the type of material flowing. External power is required to operate the regenerative components including the oxygen generation system (OGS), water recovery system (WRS), and the variable configuration carbon dioxide removal (VCCR) system. Gaseous flows are generally mixed air streams of various quality, other than the pure carbon dioxide stream exiting the VCCR. The WRS simultaneously handles both waste and gray water produced by the crew and treats the water to potable water standards. The relative quality of these water streams is not modeled. The available storage volume of all resources is sized to target the six-month mission length selected. Currently one crew member is considered, and all hardware has been sized accordingly. The crew exchanges gases directly with the crew environment, which models the interior volume of the habitat; water and food are taken directly from the appropriate stores. A parallel configuration with standby components is similarly illustrated in Fig. 5 where the standby components are connected using dashed lines with perfect switches.

Some system level assumptions are designed and applied to all reliability prediction. Most importantly, component failure is assumed to be independent. Components in the system have two states, UP and DOWN. Performance degradation is not currently under consideration. The habitat environment can provide enough resources for the crew member to survive for 60 days (1440 h). All components are nonrepairable and no preventive maintenance is provided. System failure is determined by component reliability function in RBD and MRBD, while for simulation, it is determined by crew survival conditions. During simulation, failed unit processes no longer consume or produce resources. This may cause some malfunctions to be observed as resources are not provided down the process chain. For example, all power consumers, including the OGS, VCCR, and WRS cannot function if the power supply has failed. Note that those unit processes are still functional. This will later allow us to test parallel systems with multiple resource stores.

A. Assumptions for Component Reliability

Before assigning realistic reliability models to each of the components within the system, a preliminary experiment is conducted using

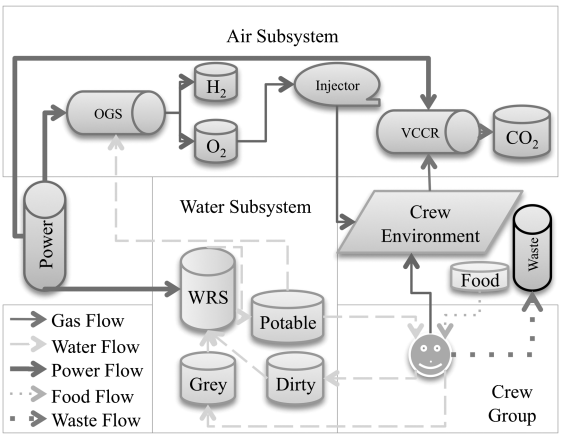

Fig. 4 Mass and power flow diagram in BioSim simulation tool.

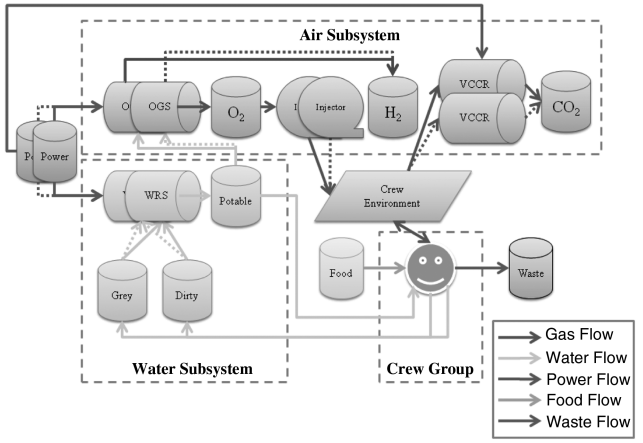

Fig. 5 Mass flow diagram for a parallel configuration in the BioSim simulation tool.

the assumption that all the components are modeled with an exponential probability density function. This test exploits the fact that the exponential reliability model is mathematically convenient for reliability analysis. The only parameter for exponential model is λ whose inverse is the MTTF. The same MTTF values are later used with more realistic probability density functions. The following section describes the assumptions made for system components, graphically represented in Fig. 6.

1. *Storage Component Reliability*

Gas and water stores are modeled with similar reliability as these tanks are similar in function and very reliable. An exponential reliability model is assigned to the storage components with an MTTF value of 8 years. The assumptions are made such that the hazard[§§] rates of the storage components remain as constants throughout the entire mission.

Resource stores for food, power and water also use exponential models, but different failure rates. Unlike the waste store, which is simply a recycling tank, the food store is considered more vulnerable due to various risks such as limited food shelf life and sensitivity to the storage environment. The power store is also more likely to fail since it faces many failure modes, for example, short circuit, overload, overheat, or blackout periods. Table 1 summarizes the design parameters for each of the storage components within the system.

2. *Regenerative Components*

When considering the reliability of regenerative components, assumptions based on previous operation of similar devices were used. The OGS is considered to be the most unreliable component within the system since there were three reported OGS failures on ISS, occurring on 8 September 2004, 1 January 2005, and 18 September 2006, respectively, during the eight-year mission. For the purpose of demonstrating the impact of component random failure on system reliability, an exponential model is selected for the OGS with a MTTF of half of the mission length.

Another important regenerative component, the WRS, consists of tubes, valves and various tanks. Most of its components are associated with increasing risks caused by repeated cyclic loads and wearout during long-term missions. Historical testing data show that although there is no recorded integrated WRS failure, many of its components have to be replaced due to performance degradation and water leakage. A two-parameter Weibull model is thus selected for the WRS to exhibit the hazard rate variation over time. The VCCR, on the other hand, is much more reliable. A normal model is assumed

[§§]Hazard rate, or hazard function $h(t)$, is the conditional probability of failure in the interval t to $t + \delta t$, given that there was no failure at t. It is expressed as $h(t) = \frac{f(t)}{R(t)}$.

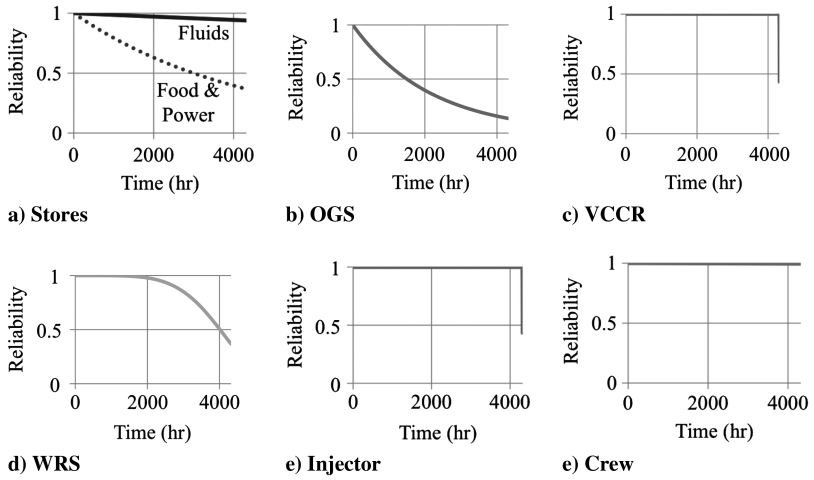

Fig. 6 Assumptions for component reliability.

for the VCCR. Table 2 summarizes the design parameters for each of the regenerative components included in the system.

3. Control Components

The injector in the system is designed to transfer oxygen from the storage tank and inject it into the habitation environment to adjust oxygen and carbon dioxide partial pressures. The injector undergoes repeated cyclic loads, therefore, a MTTF value of 90% of the desired mission length is assigned with a Normal model. This suggests that the injectors are generally less reliable than the WRS, although strictly speaking this choice is arbitrary. Table 3 shows the parameters selected for the reliability function of the control components.

4. Crew Members

The crew members are considered to be very reliable, although they are still subject to failures. Thus, since a crew failure will impact the system, just as any other unit process, a crew failure rate model has been incorporated. The failure rate model is based on previous work by Horneck and Comet [20], a linearly decreasing reliability function, which degrades from 1 to 0.9953 in 180 days. Table 4 shows the parameters selected for the crew reliability function.

Table 1 Storage component reliability assumptions

Component	Model	λ	MTTF
O_2 Store	Exponential	0.0000145	69,120 h
CO_2 Store	Exponential	0.0000145	69,120 h
H_2 Store	Exponential	0.0000145	69,120 h
Potable Water Store	Exponential	0.0000145	69,120 h
Dirty Water Store	Exponential	0.0000145	69,120 h
Grey Water Store	Exponential	0.0000145	69,120 h
Waste Store	Exponential	0.0000145	69,120 h
Food Store	Exponential	0.000231	4320 h
Power Store	Exponential	0.000231	4320 h

Table 2 Regenerative component reliability assumptions

Component	Model	λ	μ	σ	β	MTTF
OGS	Exponential	0.00046	–	–	–	2160 h
WRS	Two-parameter Weibull	0.00023	–	–	3	4320 h
VCCR	Normal	–	4320	5	–	4320 h

Table 3 Control component reliability assumptions

Components	Model	μ	σ	MTTF
Injector	Normal	3888	3	3888 h

5. Buffering Capacity Models

The buffering capacity failure models are modeled via the normal distribution. The parameter μ, representing buffering capacity, is selected to be 1440 h with a standard deviation of 1. Physically this represents oxygen remaining in the atmosphere and water remaining in storage available to the crew upon failure of the air and water revitalization subsystems. These parameters approximate an MTTF of one third of the length of the baseline mission and is selected from the perspective of system survivability in Martian missions, where 60 days would provide the crew ample time to diagnose and mitigate system upsets. A sensitivity analysis of the results considering the impact of the size of this buffer is provided in Sec. IV.A.5.

IV. Results and Discussion

Results describing the performance of each reliability prediction method are discussed in the following order: RBDs, MRBDs, MTTF, and MC with MLE. This is followed by a discussion regarding the sensitivity analysis of the environmental buffer.

A. Reliability Prediction

1. Reliability Block Diagrams

The baseline RBD approach is first tested via theoretical derivation and stochastic simulation, using Excel and MATLAB, respectively. This validation of the stochastic approach against theory is performed to provide confidence in more complicated experiments, where stochastic simulation becomes the only viable approach for reliability prediction. System reliability over time was first computed in Excel using the assumed component reliability functions; MATLAB simulations were conducted using a tool we have named the *FailureDecider*, which determines component status, functional or failed, at any given time by applying random numbers to the distribution functions described in Sec. III.A [15]. System failure data was collected and processed using the MLE method.

An exponential fit was determined to be superior to Normal and Weibull models. This was due to the quality of the fit observed relative to the other distributions, across all scenarios. This practice has been maintained throughout the case study and results in a similarly shaped curve in all analyses. This facilitates comparison of

Table 4 Crew reliability assumptions

Components	Model	Slope
Crew	Linear	-1.09×10^{-6}

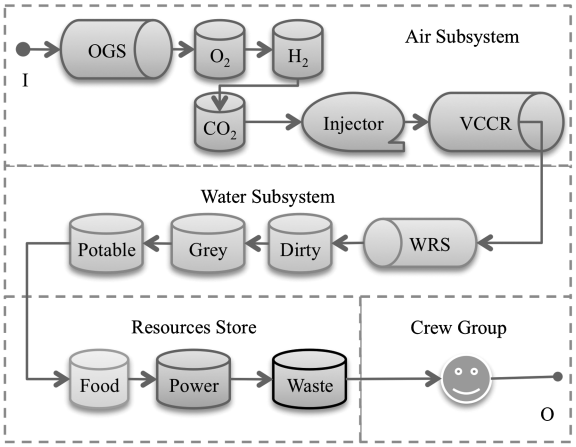

Fig. 7 Reliability block diagram for ECLSS without buffering capacity.

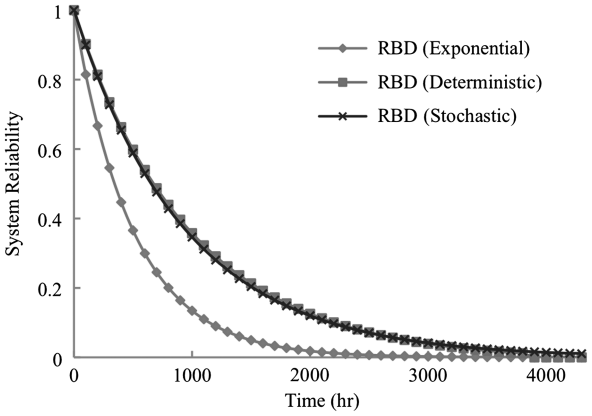

Fig. 8 Reliability prediction results from the RBD approach.

results across the various scenarios. Figure 7 illustrates the simplified system whose components are connected in series.

The reliability prediction results are presented in Fig. 8. Given an exponential fit, Eq. (9) was used for reliability prediction. It can be observed that the RBD approach using an exponential model for all components is outperformed by those using the various reliability models assumed above. This is because given the same MTTF, the reliability of exponential model degrades faster early in the life cycle as compared with normal or Weibull models. It is also shown that the reliability prediction results obtained from deterministic calculations and MATLAB simulations are consistent with each other. This

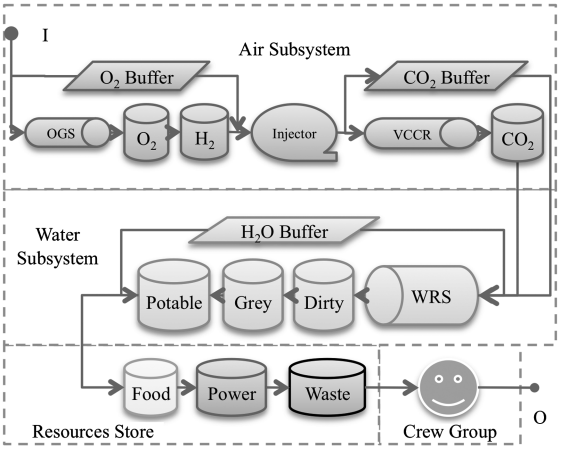

Fig. 9 Modified reliability block diagram for ECLSS with several buffers.

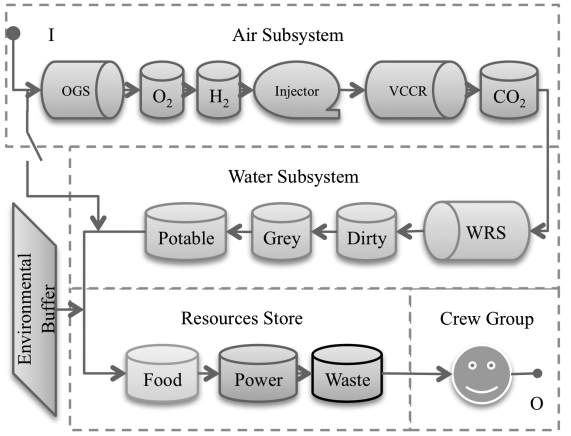

Fig. 10 Modified reliability block diagram for ECLSS with one buffer.

provides credibility to the FailureDecider tool. Lastly, it should be noted that the system reliability becomes rather low near the end of the mission.

2. Modified Reliability Block Diagrams

The second approach employed is the proposed MRBD method designed for modeling the impact of buffering capacity in reliability prediction. The key distinction is the introduction of buffers for each regenerative subsystem, or the entire system, as is illustrated in Figs. 9 and 10, respectively.

The reliability prediction results for both scenarios are based on simulation since the reliability models in a parallel-series configuration can be cumbersome for mathematical derivation. The FailureDecider tool was once again used for simulating component random failures [15]. The system failure time, taken at the end of mission, was recorded for 100 stochastic system simulations. Those data were analyzed using MLE to determine the exponential parameter capable of predicting system reliability. Again, Eq. (9) was used to display the results presented in Fig. 11, which demonstrates the difference between RBD and MRBD in reliability prediction. The MRBD prediction results are consistently higher than the RBD approach. The dashed lines represent the 95% confidence interval of the predicted system reliability over time, based on the observed variance in the data used to determine the MTTF. This confidence interval also represents the tight fit of the data modeled by the exponential distribution. The overlap of the confidence intervals suggests that these models are very similar in reliability and may be interchangeable. Interestingly, systems with buffering capacity have a reliability less than one, even at times less than the buffer MTTF. This is due to the nature of the exponential function selected [Eq. (9)], where reliability is one only at time zero.

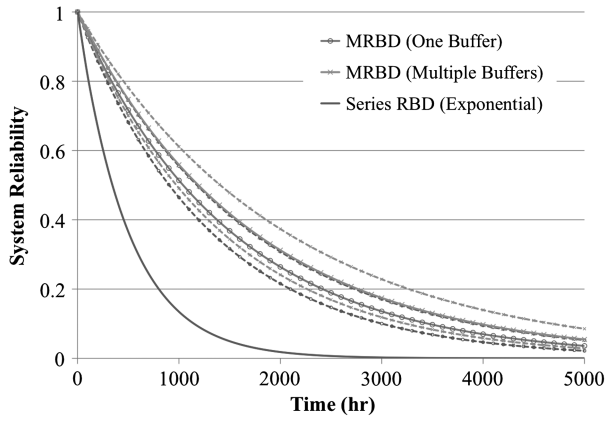

Fig. 11 Reliability prediction results from the RBD and MRBD approaches.

3. Mean Time to Failure Approach

The system MTTF (T_{sys}) for the Lunar Outpost ECLSS can be expressed in terms of component or subsystem MTTF. For the ECLSS configuration with one buffer for the air and water regeneration subsystems, the estimated system MTTF can be expressed as follows

$$T_{sys} = \min\{[T_{buffer} + \min(T_{air}, T_{water})], T_{food}, T_{waste}, T_{power}, T_{crew}\} \quad (10)$$

On the other hand, if the ECLSS configuration has multiple buffers for each regenerative subsystem, each buffer is equivalent to a standby parallel subsystem. Thus, the equation for calculating the estimated system MTTF becomes

$$T_{sys} = \min\{(T_{air_{buffer}} + T_{air}), (T_{water_{buffer}} + T_{water}), T_{food}, T_{waste}, T_{power}, T_{crew}\} \quad (11)$$

Given the assumptions for each component both Eqs. (10) and (11) results in 3600 h for both configurations. This is effectively controlled by the reliability of the air revitalization subsystem and the buffering capacity of the system. In each of the above cases $T_{buffer} = T_{air_{buffer}} = T_{water_{buffer}} = 1440$ h, as specified in Sec. III.A.5. $T_{air} = 2160$ h, where the OGS has the minimum MTTF in this subsystem. The sum of these two define the 3600 h MTTF. The next subsystems that would control MTTF given improvement in either buffering capacity or the air subsystem would be the power and food storage, which begin controlling at 4320 h, and the water revitalization subsystem and the related buffer, which begins controlling at 5760 h.

To facilitate comparison of the estimated system MTTF with the simulation approach, the results obtained above are assumed to define the parameters of an exponential system. Note, however, that the MTTF assumed for the buffering capacity is based on the designed size of the buffer assumed at time zero. When a failure occurs, however, the actual mass of material stored in the buffer is not likely to be the same as at time zero, despite the use of regenerative technologies. This leads to overprediction of system reliability (Fig. 12).

4. Monte–Carlo Style Simulation with Maximum Likelihood Estimation

The simulation tool, BioSim, is used to perform destructive life testing and to generate system failure data. These data were then processed using MLE to assess the parameters for the exponential model that describes the system reliability. As described previously, Figs. 4 and 5 depict the mass flow of the simulated series and parallel systems correspondingly. The system is subject to failure only when the crew member can no longer survive. The crew survival conditions are bound by food, water, and oxygen availability, and carbon dioxide concentration. The crew is assumed to be capable of living without food for three weeks and without water for two days. The oxygen concentration limit takes into account both an upper bound where increased fire risk occurs and a lower bound where insufficient oxygen is available for crew respiration. The carbon dioxide concentration is limited for carbon dioxide toxicity. An illustrative example regarding system failure modes is discussed in Sec. IV.B.

The reliability prediction results shown in Fig. 12 exhibit that the average MTTF obtained using the simulation tool is approximately 27 times higher than those from RBD and 4 times higher than those from MRBD. The parallel configuration improves MTTF by 20%, while the MTTF approach consistently overpredicts simulated system MTTF by approximately 7–8%.

It is believed that the simulation approximates system dynamics more accurately, and therefore, the difference in reliability prediction results validated the concerns raised previously. It is clearly demonstrated that RBD, MRBD and MTTF approaches have limited ability in modeling and predicting reliability for complex systems and they tend to either underestimate reliability for systems with buffering capacity or overestimate reliability due to inaccurate description of the buffering capacity. However, the marked improvement using the MRBD and MTTF approaches is observed by taking the buffering capacity into consideration.

5. Sensitivity Analysis

A sensitivity analysis was implemented, varying the size of the environment, to consider the impact of buffering capacity on system MTTF (Fig. 13). The horizontal axis represents seven different environmental buffer sizes, in terms of MTTF. The vertical axis defines the range of corresponding system MTTFs obtained using the MRBD method (diamonds), and the MTTF method (circles). It is suggested that the MTTF and MRBD techniques may be used to define a confidence interval bounding the actual system MTTF.

The results indicate that the predicted system MTTF upper bound has a ceiling of 4320 h, limited by the power and food storage MTTF in the current systems design. The lower bound, however, continues to increase with increasing buffering capacity. Overall, the magnitude of the range of the confidence interval increases with buffer size, until the power and food storage systems limit the increase in the upper bound.

B. System Failure Modes

A wide range of failure modes have been observed for the ECLSS under investigation. The most frequently observed failure is the air subsystem failure, where the carbon dioxide concentration exceeds tolerance limits and terminates the simulation. Failures in food and water systems have also been observed. An example failure event is presented below to demonstrate how system failure can occur in the BioSim simulation tool. Figures 14–16 are the plots representing sensor data collected during the simulations. Those data describe the inputs and outputs of the regenerative hardware components, the storage levels of various resources, and the environmental conditions

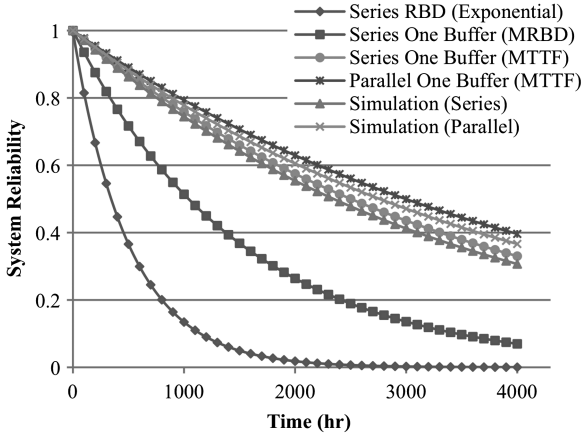

Fig. 12 Reliability prediction results from the RBD, MRBD, MTTF, and simulation approach.

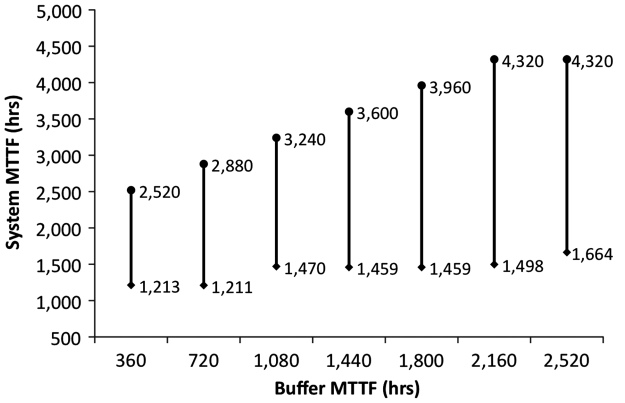

Fig. 13 The impact of varying the environmental buffer volume on system reliability.

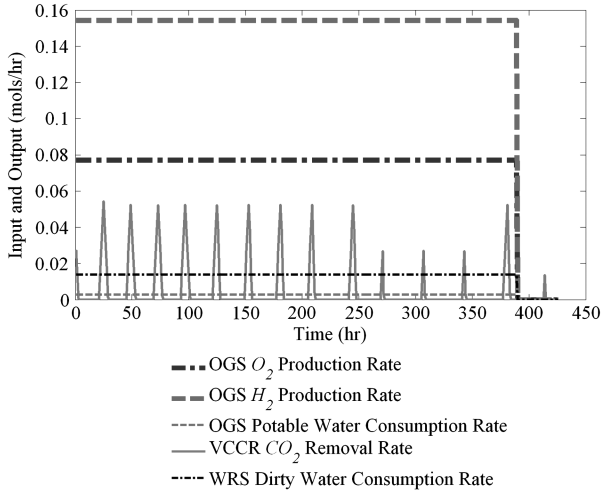

Fig. 14 I/O Sensors.

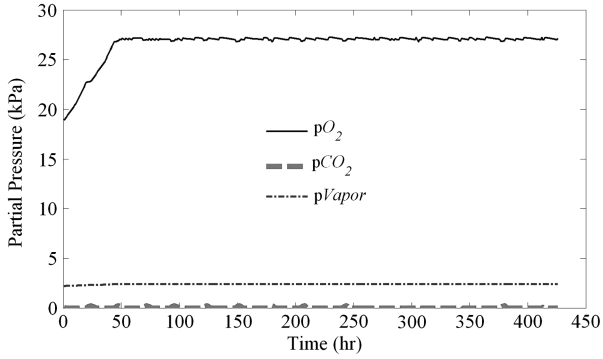

Fig. 15 Environmental condition sensors.

for crew habitation. It is by studying typical failure modes, such as those illustrated by the modeling tool, that system designers are presented with an opportunity to improve system design. With this implementation of BioSim, designers are provided an opportunity to better understand the impact of individual components on system performance and the potential for improving system reliability. The model also provides critical evidence of the buffering capacity within ECLSS, which allows the system to continue operating until the buffer is exhausted. The current results suggest that one can define an upper bound for system reliability by using the MTTF approach, however, these results may be deceptive when choosing which buffer to augment to maximize system reliability.

In this example a system failure is caused by the water subsystem. In Fig. 14, we see the oxygen production rate suddenly drops to zero after 389 h of operation. One may initially conclude that an OGS failure must have occurred, however, Fig. 15 shows that the OGS is not the cause for the system failure since the injector maintains the oxygen and carbon dioxide concentrations after the malfunction. The actual cause for the system failure is identified by considering Fig. 16, where the potable water storage level drops to zero due to a failure in the potable water store. Component random failures in BioSim are assumed to cause zero input and output, whereas storage failures cause tank levels to become zero instantly. Therefore, because there is no potable water available for OGS to produce oxygen, the production rate becomes zero at 389 h. The system failure, however, is due to the fact that the crew's potable water demand could not be satisfied and the mission comes to an end 48 h later.

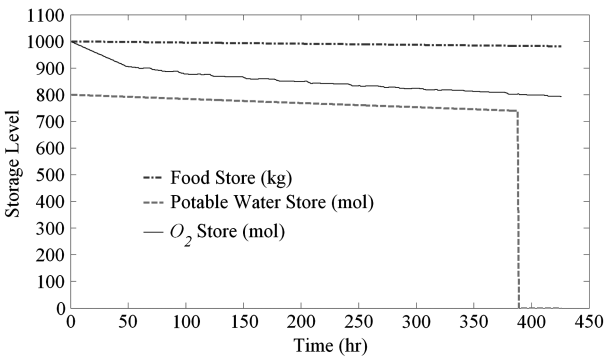

Fig. 16 Store level sensors.

V. Conclusions

This paper demonstrates the use of several approaches for studying the reliability of life-support systems in long-term space missions. The comparison between the prediction results shows a significant difference between classical and simulated approaches, which is believed to be caused by the unique characteristics of environmental systems. Classical reliability theory focuses heavily on the operational state of individual components. This is due to the original application area of reliability engineering in logistics. This ignores the potential impact that the environment can have on the function of the system. There is no doubt that life-support hardware enables the work of the crew, but system success or failure may be decided by the ability of the crew to perform, rather than strictly focusing on the ability of hardware to function. Experiments have been designed to show the inherent impact of environmental buffering capacity on system reliability and examples are given to illustrate how the system performs from this perspective. An approach using the predicted mean time to failure of individual subsystems has been proposed here, and although it overpredicts system reliability slightly, the accuracy is improved. These results depend highly on the system design assumptions the analyst selects, thus a sensitivity analysis has been prepared showing the behavior of system MTTF as the buffer MTTF is adjusted. As expected, when the environmental buffers are reduced, the bounds on systems reliability are similarly reduced. Future system designs can now be improved by this information; if the designer is confident in their selection of what the controlling buffer to their system may be, systems may be designed with reliability performance as a design constraint. In the life-support systems considered here the controlling buffer was shown to be the available oxygen in the atmosphere.

Thus, for a system designer, this work should lead toward a new perspective on design. Given a classical approach to reliability prediction, and the observed underprediction, there is either an opportunity to greatly reduce system cost by reducing the buffering capacity provided to the crew, or there is an opportunity to use the time available after malfunctions to repair failed components. This amount of time is not trivial, and given adequate resources it is expected that the crew will have ample time to diagnose a wide variety of system malfunctions and fabricate solutions. However, a system designer needs to have a strong command of the system dynamics to understand what resources will become most limiting for the crew in the event of failures. Without such understanding, it is not necessarily obvious exactly which buffer should be augmented in size, where to perform preventive versus corrective maintenance, or where to provide redundancy.

Acknowledgments

The authors would gratefully like to acknowledge the generosity of the University of Illinois, the National Aeronautics and Space Administration, the National Science Foundation, and the Illinois Space Grant Consortium in support of this work. The authors would also like to thank several individuals who also contributed to this work, particularly Izaak Neveln, David Kane, and Christian Douglass, who supported this work while partaking in an National Science Foundation Research Experience for Undergraduates.

References

[1] Perera, J., and Field, S., "Integrated Risk Management Application (IRMA)," *NASA Risk Management Conference*, NASA Johnson Space Center, Houston, TX, 2005.

[2] Leveson, N., *Safeware*, Addison Wesley Longman, Reading, MA, 1995.

[3] Lievens, C., *System Security*, Caepadues Editions, Toulouse, France, 1976.

[4] Anonymous, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems," IEEE Publications, Piscataway, NJ, 1975.

[5] Yamada, K., "Reliability Activities at Toyota Motor Company," *Reports of Statistical Application Research, Union of Japanese Scientists and Engineers*, Vol. 24, No. 3, 1977.

[6] Fussel, J. B., "Fault Tree Analysis-Concepts and Techniques," Vol. E, Univ. of Liverpool, Liverpool, UK, 1973.

[7] Pages, A., and Gondran, M., *System Reliability Evaludation & Prediction in Engineering*, Springer–Verlag, 1st ed., New York, 1986.

[8] Kletz, T., *Hazop and Hazan*, Taylor & Francis, 4th ed., Washington, D.C., 1999.

[9] Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures, with Worked Examples*, Wiley-AIChE, 2nd ed., New York, 1992.

[10] Vesely, W. E., Goldberg, F. F., Roberts, N. H., and Hassel, D. F., *Fault Tree Handbook*, U.S. Nuclear Regulatory Commission, Washington, D.C., 1981.

[11] O'Connor, D. T., Newton, D., and Bromley, R., *Practical Reliability Engineering*, Wiley, 4th ed., West Sussex, England, 2002.

[12] Kortenkamp, D., and Bell, S., "BioSim: An Integrated Simulation of an Advanced Life Support System for Intelligent Control Research," *International Conference on Environmental Systems*, SAE, Warrendale, PA, 2003.

[13] Rodríguez, L. F., Bell, S., and Kortenkamp, D., "Using Dynamic Simulations and Automated Decision Tools to Design Lunar Habitats," *International Conference on Environmental Systems*, SAE, Paper No. 2005-01-3011, 2005.

[14] Rodríguez, L. F., Jiang, H., Bell, S., and Kortenkamp, D., "Testing Heuristic Tools for Life Support System Analysis," *International Conference on Environmental Systems*, SAE, Paper No. 2007-01-3225, 2007.

[15] Jiang, H., Bhalerao, K., Soboyejo, A., Bell, S., Kortenkamp, D., and Rodríguez, L. F., "Modeling Stochastic Performance and Random Failure," *International Conference on Environmental Systems*, SAE, Paper No. 2007-01-3027, 2007.

[16] Rodríguez, L. F., Bell, S., and Kortenkamp, D., "Use of Genetic Algorithms and Transient Models for Life Support Systems Analysis," *Journal of Spacecraft and Rockets*, Vol. 43, No. 6, 2006, pp. 1395–1403.
doi:10.2514/1.18232

[17] Klein, T., Subramanian, D., Kortenkamp, D., and Bell, S., "Using Reinforcement Learning to Control Life Support Systems," *Proceedings of the International Conference on Environmental Systems*, SAE, Warrendale, PA, 2004.

[18] Kortenkamp, D., Izygon, M., Lawler, D., Schreckenghost, D., Bonasso, R. P., Wang, L., and Kennedy, K., "A Testbed for Evaluating Lunar Habitat Autonomy Architectures," *Proceedings of the 6th Conference on Human/Robotic Technology and the Vision for Space Exploration in the Space Technology and Applications International Forum (STAIF)*, Vol. 969, American Institute of Physics Conference Proceedings, College Park, MD, 2008, pp. 741–748.

[19] Righini, R., Bottazi, A., Cobopoulos, Y., Fichera, C., Giacomo, M., and Perasso, L., "A New Monte–Carlo Method for Reliability Centered Maintenance Improvement," *International Conference on Safety and Reliability*, Vol. 3, European Safety and Reliability Association, Greece, 1996, p. 14.

[20] Horneck, G., and Comet, B., "General Human Health Issues for Moon and Mars Missions: Results from the HUMEX Study," *Advances in Space Research*, Vol. 37, No. 12006, pp. 100–108.
doi:10.1016/j.asr.2005.06.077

P. Gage
Associate Editor