Prediction of Reliability of Environmental Control and Life Support Systems

Haibei Jiang* and Luis F. Rodríguez†

University of Illinois at Urbana-Champaign, Urbana, IL, 61801, USA

Scott Bell‡ and David Kortenkamp§

NASA-Johnson Space Center, Houston, TX, 77058, USA

Francisco Capristan¶

Georgia Institute of Technology, Atlanta, GA, 30332, USA

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 exploration 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

*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 61801

†Corresponding author. Assistant Professor, Department of Agricultural and Biological Engineering, 376C Agricultural Engineering Sciences Building, MC-644, 1304 West Pennsylvania Avenue, Urbana, IL 61801. AIAA Member.

‡Research Scientist, TRACLabs Inc., 1012 Hercules, Houston, TX 77058

§Senior Scientist, TRACLabs Inc., 1012 Hercules, Houston, TX 77058. AIAA Member.

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

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

$R(t)$ system reliability

$R_i(t)$ reliability of subsystem i

$F(t)$ cumulative failure function

$f(t)$ probability density function

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.

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 function is μ.

σ one of the two characteristic parameters describing the normal distribution. Generally σ is a unitless measure of variance.

$L(X_1, \ldots, X_n; \Theta)$ the likelihood function of the system described by failure data $X_i, \ldots, X_n$, as controlled by the mean likelihood estimator Θ.

Θ the mean likelihood estimator

λ^* the predicted value of the mean likelihood estimator of the exponential distribution

n the number of data points utilized to determine the mean likelihood estimator of the exponential distribution

β a characteristic parameter of the two parameter Weibull distribution.

T_{sys} the estimated mean time to failure of the system

T_i the estimated mean time to failure of subsystem i

$\mathbf{min}(a, b, c)$ minimum function, returning the smallest value of a, b, or c

I. Introduction

Large scale complex environmental control systems, such as those considered by the National Aeronautics and Space Administration (NASA) feature non-deterministic 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 multi-degree fault tolerance and well proven contingency plans are desired by NASA and its space exploration program[a]. 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. 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[b]. 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[c]. 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

[a] See Exploration Life Support Overview available at: http://els.jsc.nasa.gov/, last accessed on December 9, 2009.

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

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

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 use of opinion from 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 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 utilized 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 availabilty 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 resouces 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:

- Provide a virtual test bed which allows mission designers to test different system designs and study the tradeoff between design and system reliability;
- Predict the reliability function for the integrated system based on component reliability functions;
- Determine the minimum component reliability requirements given various system level reliability objectives;
- Test different corrective and preventive maintenance strategies to determine the optimal maintenance scheduling;
- Compare system ESM (Equivalent System Mass) and MTTF (Mean Time To Failure);
- Address the buffering capacity in ECLSS and its impact on system reliability and cost.

Due to 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: Section II introduces the reliability prediction approaches adopted for this analysis, including reliability block diagram, modified reliability block diagram, simulation experiments and statistical methods; Section III describes a simplified life support system in a 180-day Lunar Outpost mission and discusses the experimental results obtained for this system; Section IV presents the conclusions and the directions for future research.

II. Methodology

A. Reliability Modeling and Prediction Approaches

Four reliability prediction methods and the reasoning behind their seledction will be discussed in this section. These methods include 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).

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 Figure 1 where

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

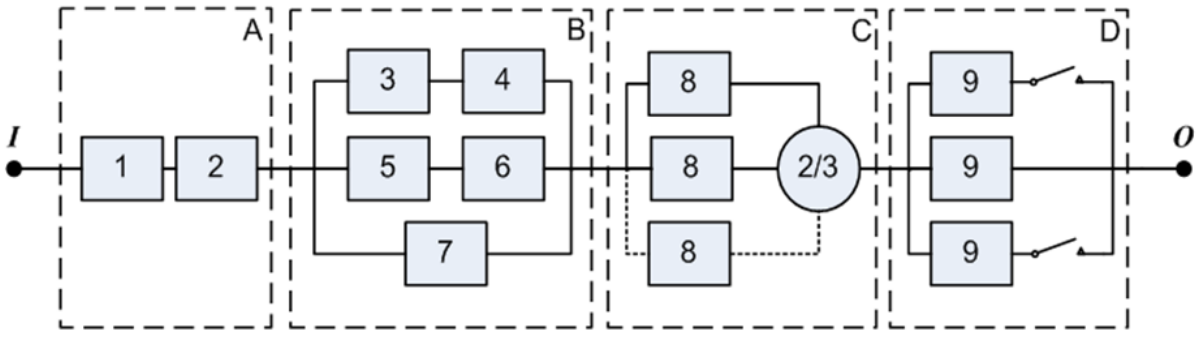


Figure 1. Reliability Block Diagrams

In conventional reliability theory, the integrated system is in its 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,

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

For parallel systems, the reliability function is,

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

The generalized *k-out-of-n* system, 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,

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

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 until time t and the probability that the primary unit fails at some time τ, $0 < \tau < t$ while the standby unit functions successfully from τ to time t. Mathematically,

$$R(t) = R_1(t) + \int_{\tau=0}^{t} f_1(\tau)R_2(t-\tau)dt, \tag{4}$$

where $R_1(t)$ and $R_2(t)$ denote the reliabilities of the primary unit and the standby unit at time t respectively, and $f_1(t)$ is the probability density function of 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 multi-unit standby system is given by

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

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. First of all, conditional component failure probability functions need to be determined, and independent component failures need to be assumed. Secondly, the components in the system need to have a linear relationship with specified inputs and outputs. A reasonable approximation is to use mass flows as component inputs and outputs. Lastly, it is currently assumed that no preventive or corrective maintenance is available for system components since the maintenance actions will drastically change the fundamental implementation of RBD. 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 in ECLSS is caused by the fact that system failure is no longer determined by component states, rather, the crew state and their productivity is the major concern. 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 Figure 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 remaining challenge of selecting a function that physically represents the buffering capacity, and properly sizing that function, 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

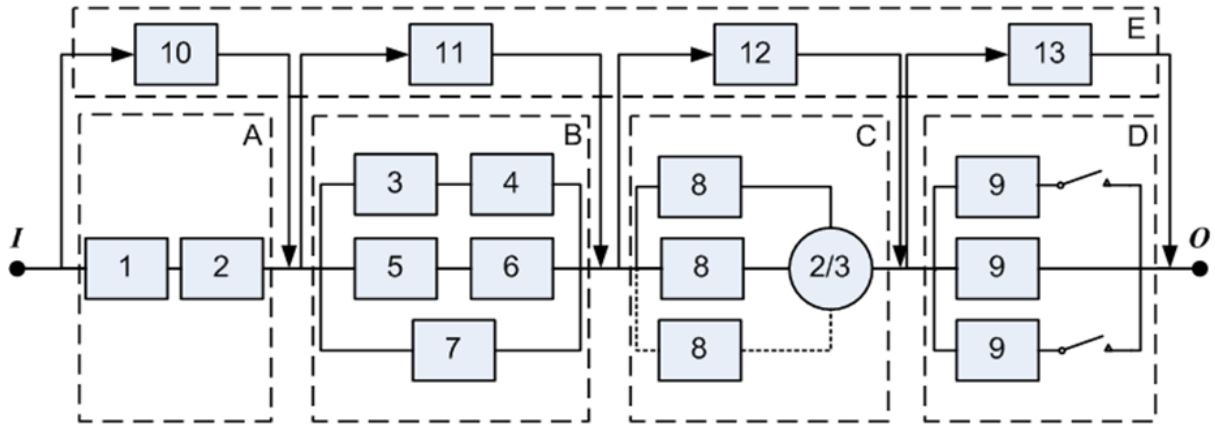


Figure 2. Modified Reliability Block Diagrams

be utilized as a system reliability indicator since the probability of system failure is one when the reliability of buffer becomes zero, which physically means the exhaustion of a critical resource. 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 Figure 3 has a very sharp reliability decrement after 4,320 hours 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

Another way to approximate system reliability is the direct use of component MTTF. This is a deterministic method based on the reliability assumptions for individual components. The core idea in this approach is to find the bound for system life time from subsystem life times by decomposition. For a series system, $MTTF_{sys} = \min\{MTTF_1, MTTF_2, \dots\}$; for a system with active redundancy, $MTTF_{sys} = \max\{MTTF_1, MTTF_2, \dots\}$; for a system with standby redundancy, $MTTF_{sys} = \sum_{i=1}^{n}\{MTTF_i\}$, where n is number of standby components. The major advantage of this approach is its convenience.

4. Monte Carlo Style Simulation with Maximum Liklihood Estimation

BioSim is a dynamic system simulation tool developed by NASA Johnson Space Center.[12–15] Mathematical models for typical components found in various life support systems are fully

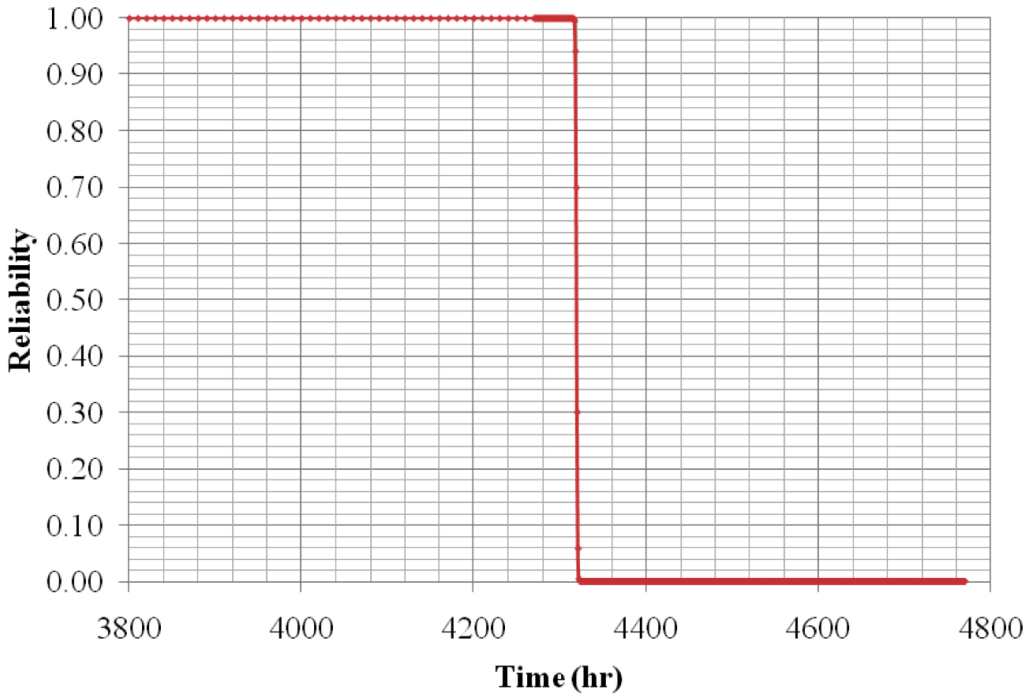


Figure 3. A normal reliability function with $\mu = 4320, \sigma = 1$.

integrated and highly configurable. Simulation progresses in hourly time increments, with each unit process producing and consuming various resources in designated stores. An Extensible Markup Language (XML) configuration file containing the design of the system initializes the simulation including settings such as random failure and stochastic performance.[16] BioSim has been successfully utilized and verified in many ECLSS design applications, including optimization,[17] reliability analysis,[16] control system testing,[13,18] and power system design verification.[19]

Monte Carlo Simulation[20] (MC) allows the analyst to consider various outcomes the system may encounter. The simulation environment we developed also enables us to study many reliability and cost related aspects 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 on 100 identical systems, whose failure time and causes are captured for reliability prediction. In our application, the major concern is that even if a numerous trials have been conducted, there's still no guarantee that we can exhaustively span the whole search space and identify all the possible 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

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

The maximum likelihood estimator (MLE) of Θ, or Θ^*, will maximizes L. In most cases, the MLE is obtained by differentiating Equation 7, setting equal to zero and solving for the unknowns. For an exponential distribution the characteristic variable is the failure rate λ, and the MLE is determined by taking the reciprocal of the mean of the failure times as in Equation 8.

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

where x_i is the time of the i^{th} failure and the 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 utilizing this approach.

Parameters identified can be subsequently utilized to predict reliability, $R(t)$. In the case of the exponential distribution the the form of the reliability function is as in Equation 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 envionment 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 days 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 is used to predict the lower bound for system reliability and it treats the buffering capacity as if it's a parallel resource component. The MTTF approach is considered to be more optimistic and therefore, it is used to predict the upper bound for system reliability. Observed MTTF is reported and shown to be within each of the two bounds on the system.

III. Case Study

The objectives of the case study presented here are as follows:

1. Develop a software application where various reliability modeling and prediction approaches can be performed and compared;

2. Utilize the application to study a representative example and compare the difference between the reliability prediction results;

3. Discuss the cause of deviation in reliability prediction results and its impact on system design and operation.

A. Life Support System for Lunar Outpost

The ECLSS tested in this project is designed for a six-month Lunar Outpost mission. It consists of four types of components: *bulk storage components* (i.e. gases and water), *regen-*

erative components (i.e. Oxygen Generation System and Water Recovery System), *control components*, and *crew members*. A typical series configuration of such a system is depicted in Figure 4, where the mass and power flow is shown. In Figure 4, horizontal cylinders represent regenerative processors and vertical cylinders represent storage units. Arrows represent the flow of mass from one unit to the next. Color coding is utilized 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, save for the pure carbon dioxide stream exiting the VCCR. The WRS handles both waste and grey water produced by the crew and produces a potable water, though the related quality of these water steams 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. However water and food are taken directly from the appropriate stores. Similarly, a parallel configuration with standby components is illustrated in Figure 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 approaches. Most important, component failure is assumed to be independent. In simulation, however, failed hardware no longer consume or produce resources. Thus, some failures may 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 resources stores. In addition, several other assumptions are held in all cases and should be made explicit:

1. Components in the system have two states, UP and DOWN. Performance degradation is not currently under consideration.

2. The habitat environment can provide enough resources for the crew member to survive for 60 days (1,440 hours).

3. All components are non-repairable and no preventive maintenance is provided.

4. System failure is determined by component reliability function in RBD and MRBD, while for simulation, it is determined by crew survival conditions.

The crew habitat failure model is modeled via the normal distribution. The parameter μ, representing buffering capacity, is selected to be $1,440$ hours with a standard deviation

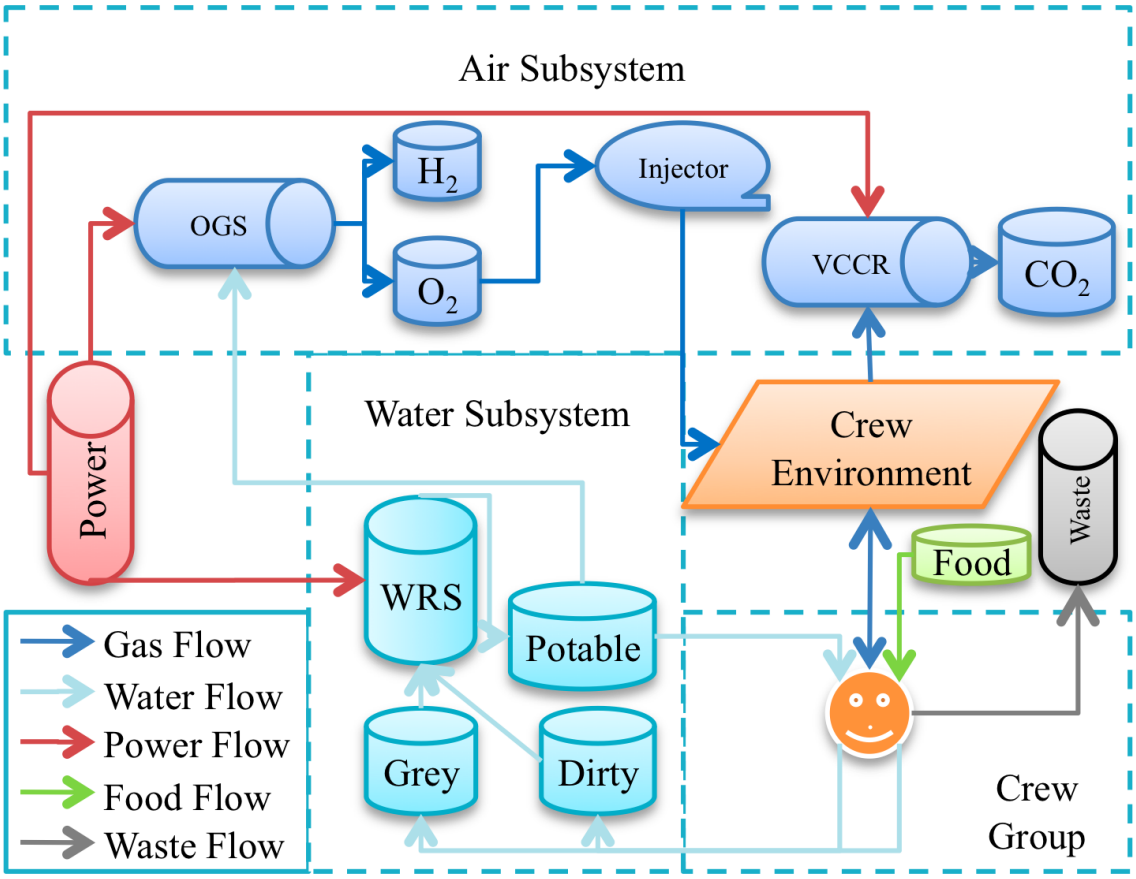


Figure 4. Mass and power flow diagram in BioSim simulation tool.

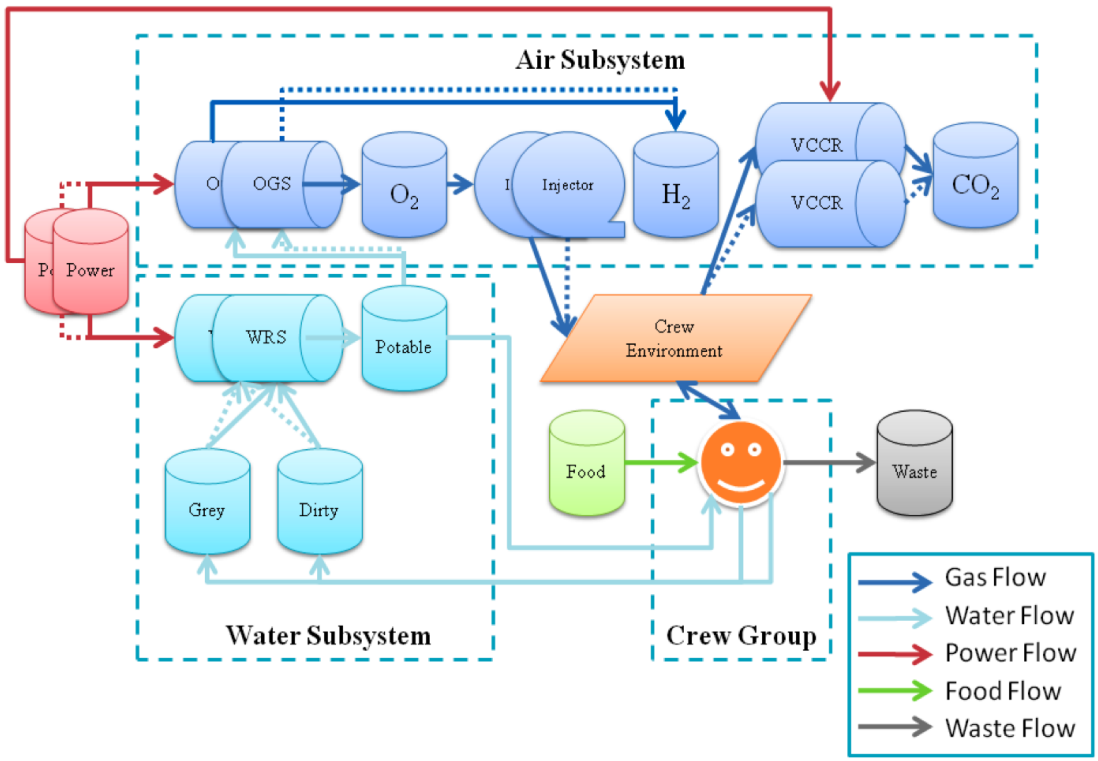
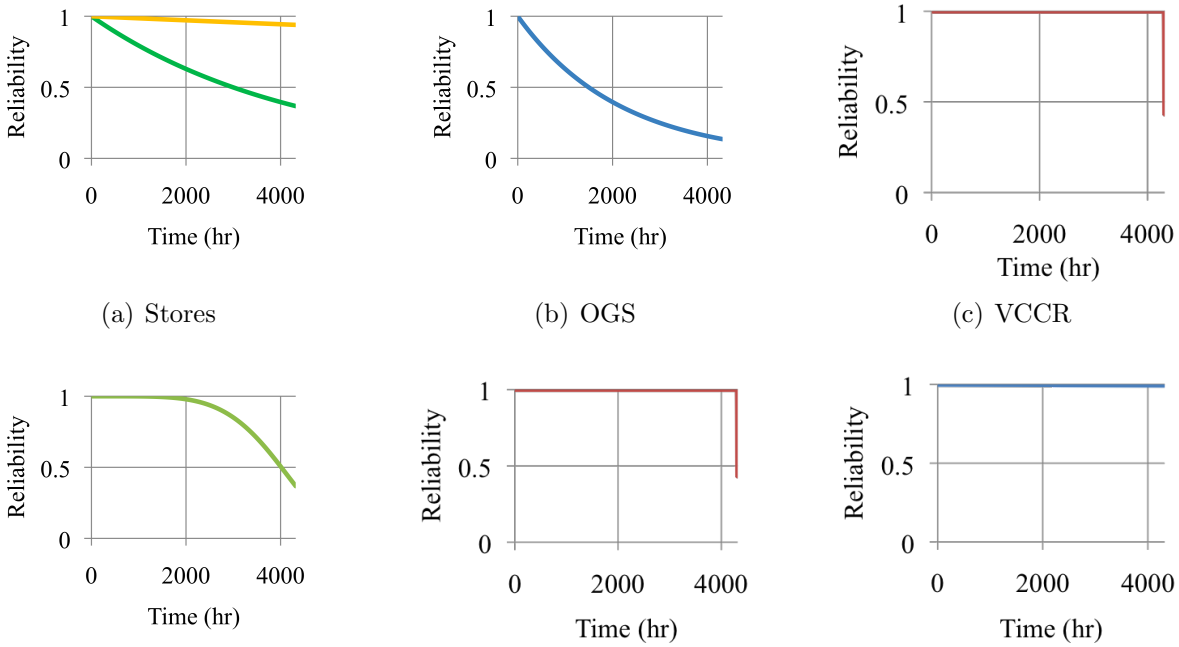


Figure 5. Mass flow diagram for a parallel configuration in the BioSim simulation tool

of 1. This is approximately 1/3 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.

B. Assumptions for Component Reliability

Before assigning realistic reliability models to each of the components within the system, a preliminary experiment is conducted using 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 utilized for more realistic probability density function assumptions. The following section describes the assumptions made for system components and the component reliability functions are graphically represented in Figure 6.



(a) Stores (b) OGS (c) VCCR

(d) WRS (e) Injector (f) Crew

Figure 6. Assumptions for component reliability.

1. *Storage Component Reliability*

Gas and water stores are modeled with similar reliabiity 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 eight years. The assumptions are made such that the hazard rates[d] 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.

Table 1. Storage component reliability assumptions.

Component	Model	λ	MTTF
O_2 Store	Exponential	0.0000145	69120 hrs
CO_2 Store	Exponential	0.0000145	69120 hrs
H_2 Store	Exponential	0.0000145	69120 hrs
Potable Water Store	Exponential	0.0000145	69120 hrs
Dirty Water Store	Exponential	0.0000145	69120 hrs
Grey Water Store	Exponential	0.0000145	69120 hrs
Waste Store	Exponential	0.0000145	69120 hrs
Food Store	Exponential	0.000231	4320 hrs
Power Store	Exponential	0.000231	4320 hrs

2. Regenerative Components

When considering the reliability of regenerative components, assumptions based on previous operation of similar devices was utilized to select assumptions. The OGS is considered to be the most unreliable component within the system boundary since there were three reported OGS failures on ISS, occuring on September 8, 2004, January 1, 2005 and September 18, 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 down-scaled MTTF which is 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 severe wear-out 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 in practice due to performance degradation and water leakage. A 2-parameter Weibull model is thus selected for the WRS to exhibit the hazard rate variation over time. The VCCR, on the

[d]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 $h(t) = \frac{f(t)}{R(t)}$

other hand, is much more reliable. A normal model is assumed for the VCCR so that each regenerative component has its distinct reliability model. Table 2 summarizes the design parameters for each of the regenerative component included in the system.

Table 2. Regenerative component reliability assumptions.

Component	Model	λ	μ	σ	β	MTTF
OGS	Exponential	0.00046	–	–	–	2160 hrs
WRS	Weibull 2	0.00023	–	–	3	4320 hrs
VCCR	Normal	–	4320	5	–	4320 hrs

3. Control Components

The injector in the system is designed to consume oxygen from the storage tank and inject it into the habitation environment to adjust oxygen and carbon dioxide partial pressure. 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.

Table 3. Control component reliability assumptions.

Components	Model	μ	σ	MTTF
Injector	Normal	3888	3	3888 hrs

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 failre rate model is based on previous work by Horneck and Comet,[21] 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 4. Crew reliability assumptions.

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

C. Reliability Prediction

1. *Reliability Block Diagrams*

As previously described, the system reliability has been determined using the proposed reliability prediction approaches. The 'naïve' RBD approach, since it does not take system buffering capacity into account, is first tested by theoretical derivation and stochastic simulation, using Excel and Matlab respectively. This validation of the stochastic approach against theory is performed to provide confidence for more complicated experiments where stochastic simulation becomes the only viable approach for reliability prediction. System reliability over time is first computed in Excel using the assumed component reliability functions Matlab simulations are 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 Section III.B.[16] Then system failure data is 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 across the various techniques (Figure 8). This practice has been maintained throughout the case study and results in a similarly shaped curve in all analyses, facilitating comparison of results across the various scenarios. Figure 7 illustrates the simplified system whose components are simply connected in series and will cause system failure if any one of them fails.

The reliability prediction results are presented in Figure 8, which illustrates the several different scenarios designed for the RBDs approach. Given an exponential fit, Equation 9 was utilized for reliability prection. It can be observed that the RBD approach using an exponential model for all components is outperformed by those using various reliability models. This is because given the same MTTF, the reliability of exponential model degrades faster as compared to Normal or Weibull models early in the life cycle. It is also shown that the reliability prediction results obtained from deterministic calculations and Matlab simulations are quite consistent with each other. This provides credibility for the FailureDecider tool. Lastly, it should be noticed that the system reliability becomes rather low at 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. In this experiment, the system diagram is slightly different from the naïve system representation. The major difference is the introduction of buffers for each regenerative subsystem, or the entire system, as is illustrated in Figure 9 and Figure 10, respectively.

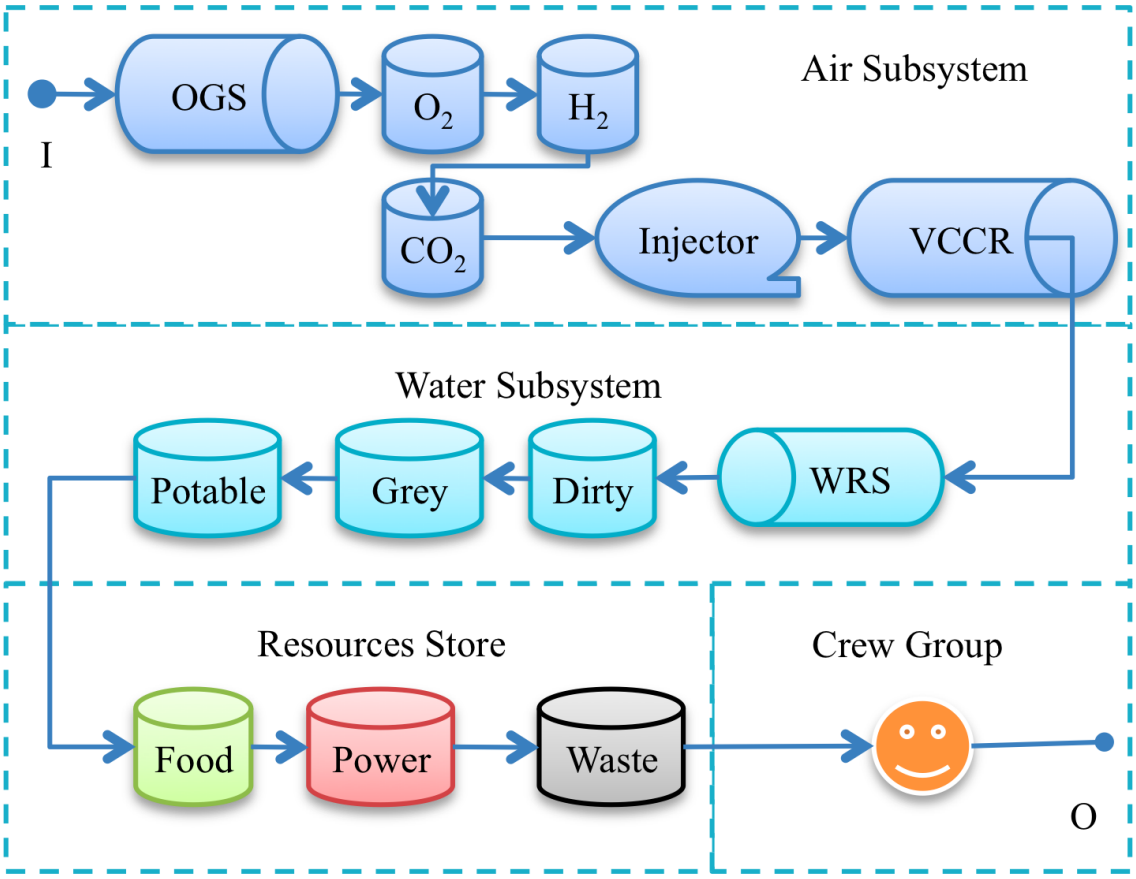


Figure 7. Reliability block diagram for ECLSS without buffering capacity.

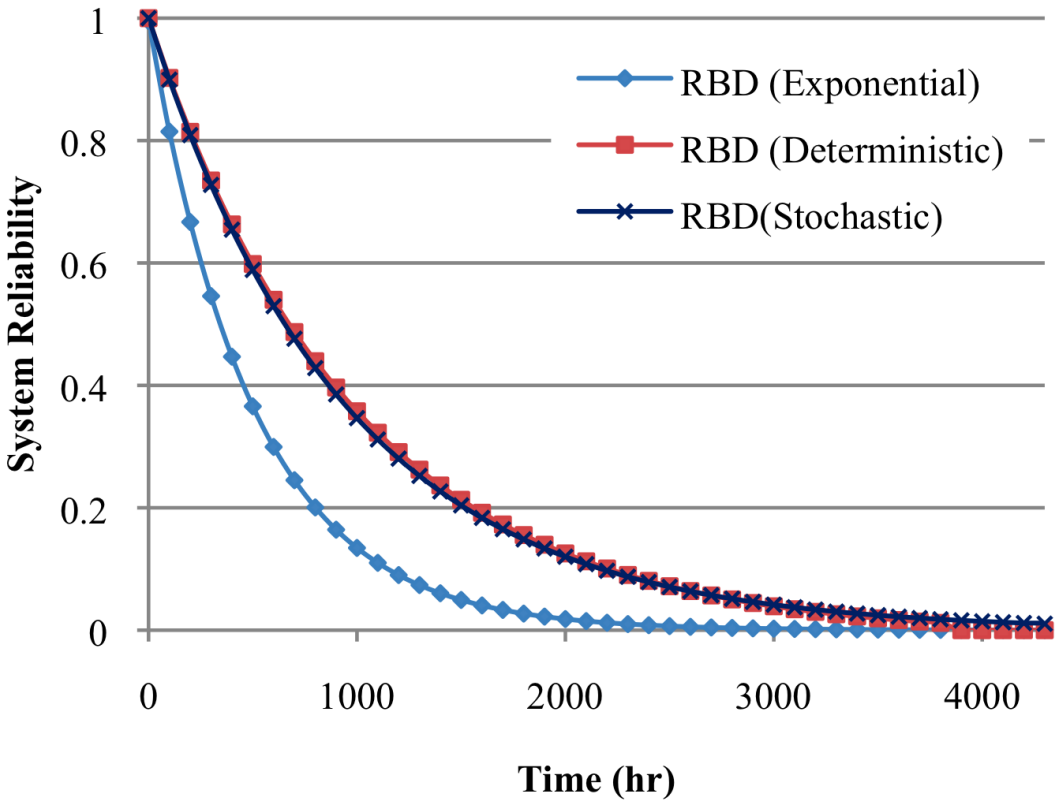


Figure 8. Reliability prediction results from the RBD approach.

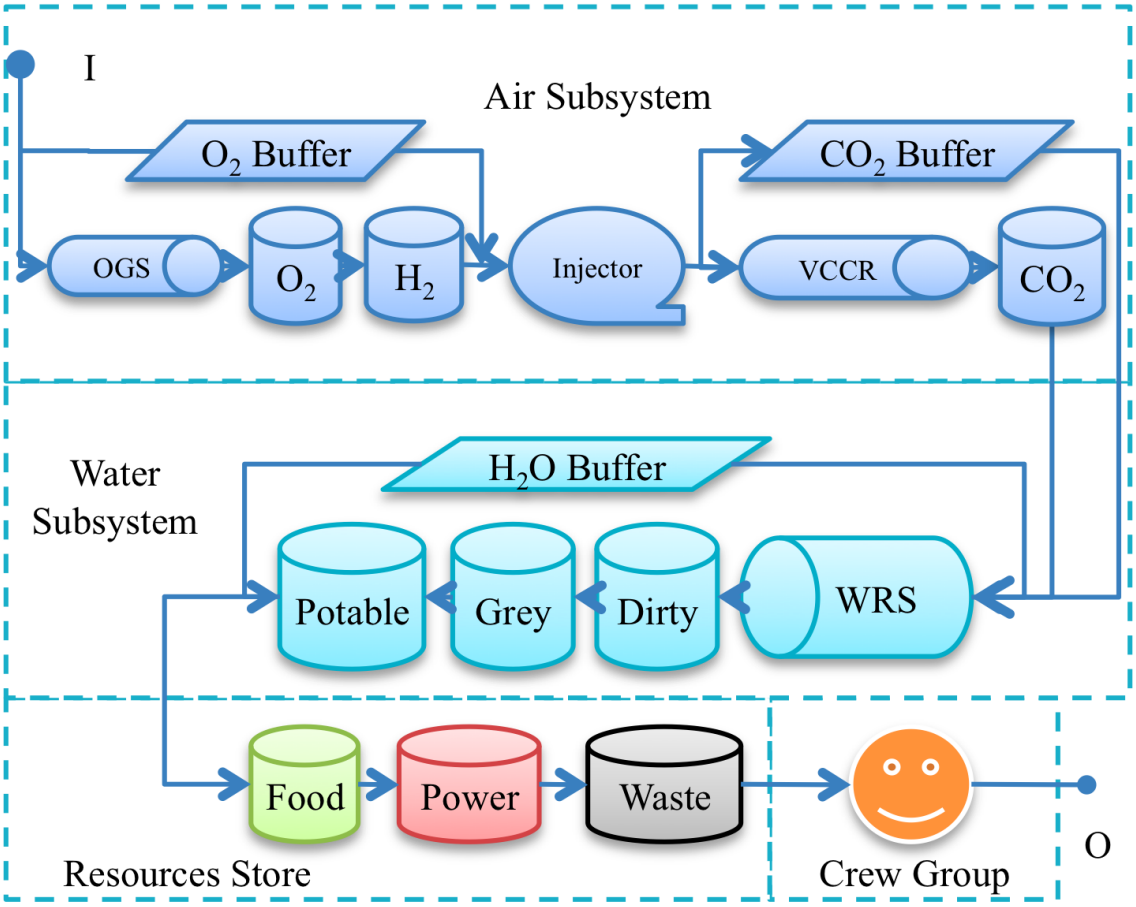


Figure 9. Modified reliability block diagram for ECLSS with several buffers.

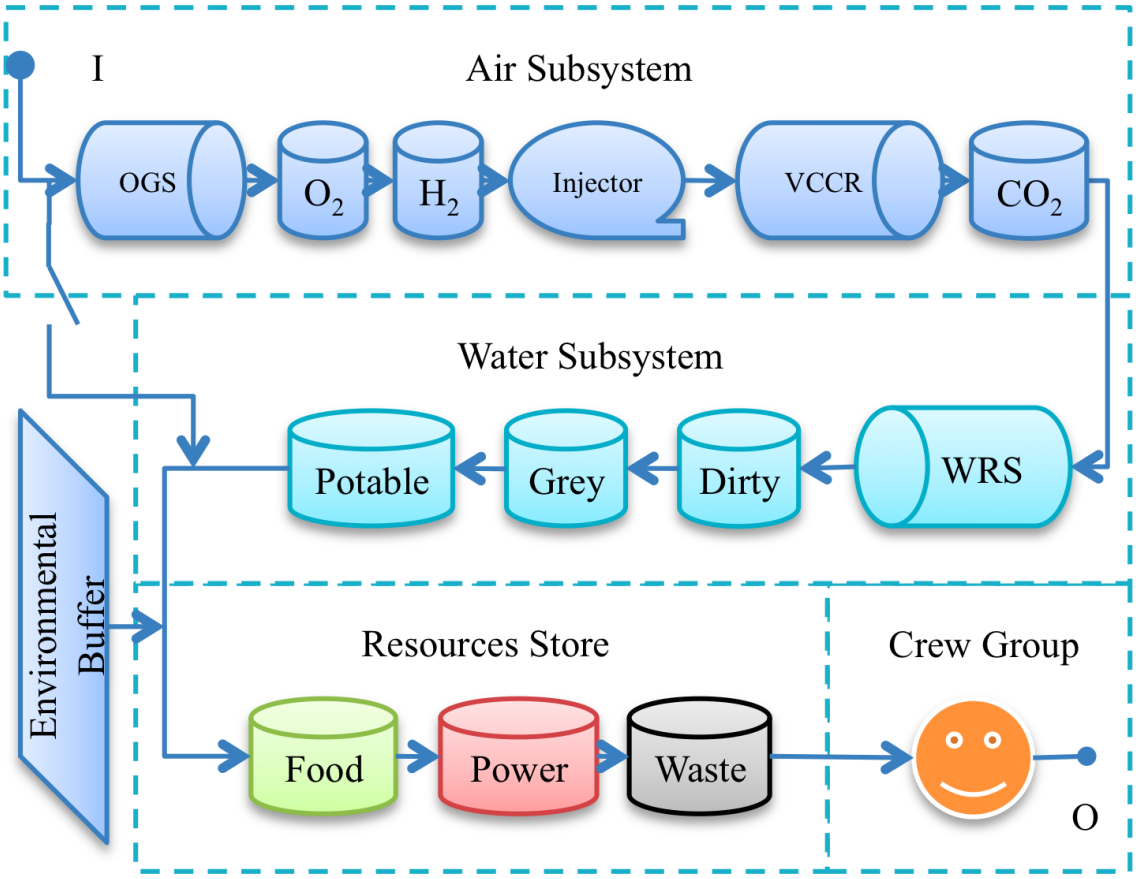


Figure 10. Modified reliability block diagram for ECLSS with one buffer.

The reliability prediction results for both scenarios are based on simulation since the reliability models in a parallel-series configuration are cumbersome for mathematical derivation. The FailureDecider tool is once again used for simulating component random failures.[16] The system failure time, taken at the end of mission, is recorded for 100 identical system configurations stochastically. Those data are analyzed using MLE to determine the exponential parameter capable of predicting system reliability and comparable with the results from the naïve series system tested using RBDs. Again, Equation 9 was utilized to display the results presented in Figure 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 the data utilized to determine of the MTTF. The overlap of the reliability prediction results of the one buffer model and the multiple buffer model suggests that these models are very similar in reliability and may be interchaneable. 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 (Equation 9), where reliability is one only at time equal to zero.

3. Mean Time To Failure Approach

The system MTTF (T_{sys}) for the ECLSS in the Lunar Outpost mission can be numerically expressed in terms of component or subsystem MTTF, for example T_{OGS} and T_{VCCR}, or, T_{air} and T_{water}. More specifically, for the ECLSS configuration that has one buffer for the entire air and water regenerative system, the estimated system MTTF can be expressed as follows,

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

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,

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

By substituting the MTTF assumptions for each component into equation 10 and 11, the results are $3,600$ hours for both configurations.

For comparing the estimated values of system MTTF with the results from the simulation approach, the results obtained above are assumed to define the parameters of an exponential system as suggested by the simplest system configurations. Note, however, that the MTTF

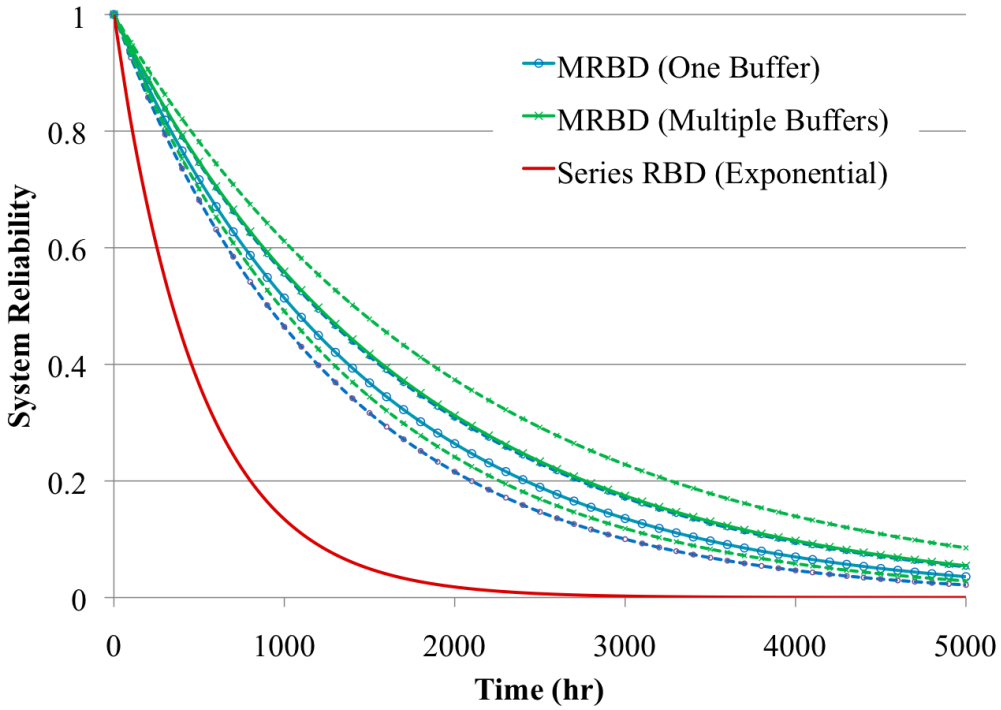


Figure 11. Reliability prediction results from the RBD and MRBD approaches.

assumed for the buffering capacity is based on the designed size of the buffer assumed at time zero. However, when a failure occurs, 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 the observed over-prediction of system reliability using this function.

4. Monte Carlo Style Simulation with Maximum Liklihood Estimation

The simulation tool, BioSim, is utilized to perform destructive life testing and generate system failure data. These data are then processed using MLE to assess the parameters for the exponential model that describes the system reliability. As described previously, Figure 4 and Figure 5 depict the mass flow of the simulated series and parallel systems correspondingly. Several additional assumptions are made for the simulation, including:

1. OGS, VCCR, and WRS require power, suggesting that if the power store is *DOWN*, all the regenerative component will not be able to consume and produce any resources despite the fact that they are still functional.

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

3. WRS has 100% conversion efficiency.

4. Crew daily schedule is: 8-hour of sleep (Intensity level of 0), 12-hour of lab work (Intensity level of 2), and 4-hour of exercises (Intensity level of 4).

5. The initial power, food, and water storage levels are designed to satisfy the requirements for the nominal mission length.

In this experiment, results are generated only using the BioSim simulation tool. The system is subject to failure only when the crew member can no longer survive and the crew survival conditions are bounded by food, water availability, and oxygen, 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. Two illustrative examples regarding system failure modes are discussed in Section III.D.

The reliability prediction results shown in Figure 12 exhibit that the average MTTF obtained using the simulation tool is approximately 27 times higher than those from RBD and four times better than those from MRBD. The parallel configuration improves MTTF

by 20%, while the MTTF approach consistently over predicts 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 all 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, marked improvement using the MRBD and MTTF approaches is observed by taking the buffering capacity into account.

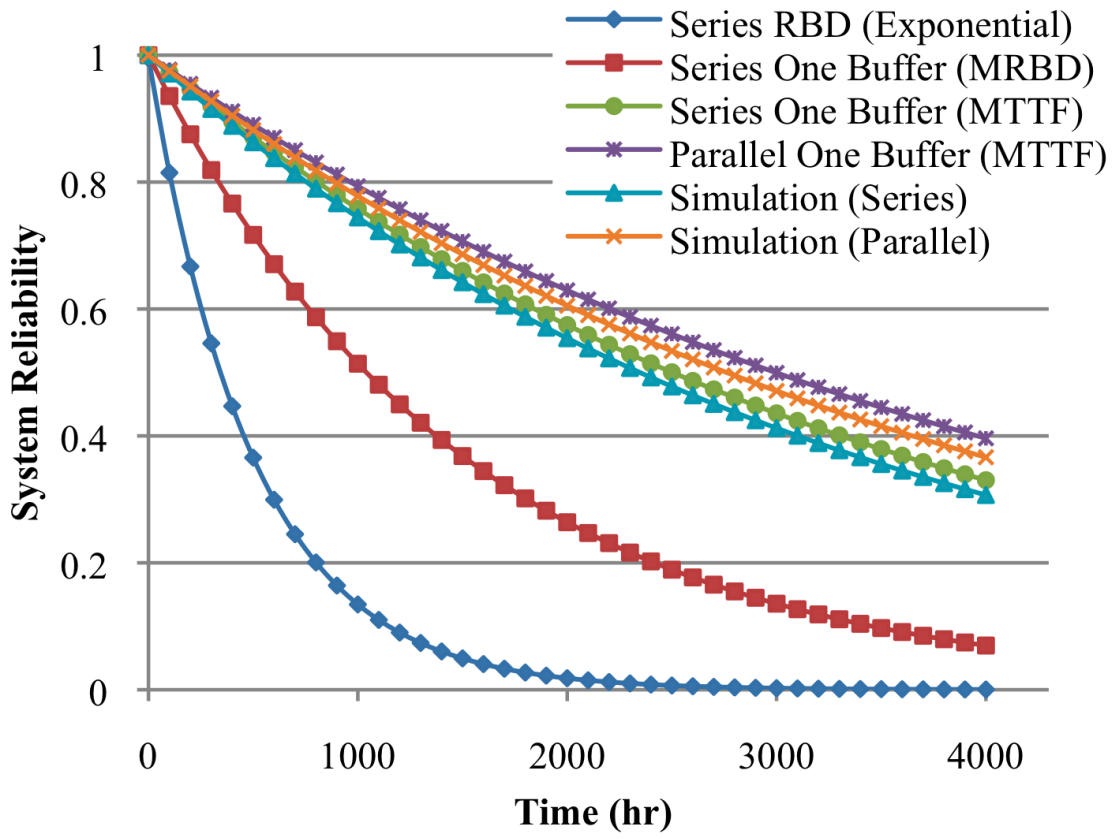


Figure 12. Reliability prediction results from the RBD, MRBD, MTTF and simulation approach

5. Sensitivity Analysis

A sensitivity analysis was implemented, varying the size of the envrionment, to consider the impact of buffering capacity on system MTTF (Figure 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, denoted by diamond dots, and the MTTF method, denoted by circles. The middle bars represent the actual system MTTFs determined via a series of 100 simulations at each level. It is suggested that the MTTF and MRBD techniques may be utilized to define a confidence interval bounding the actual system MTTF.

The results indicate that the predicted system MTTF upper bound has a ceiling of 4,320 hours, given large buffering capacity, limited by the power component MTTF in the current systems design. This is due to the effective cap on maximum MTTF imposed by the current assumptions on the power system. 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 limitations in the power system limits the increase in the upper bound.

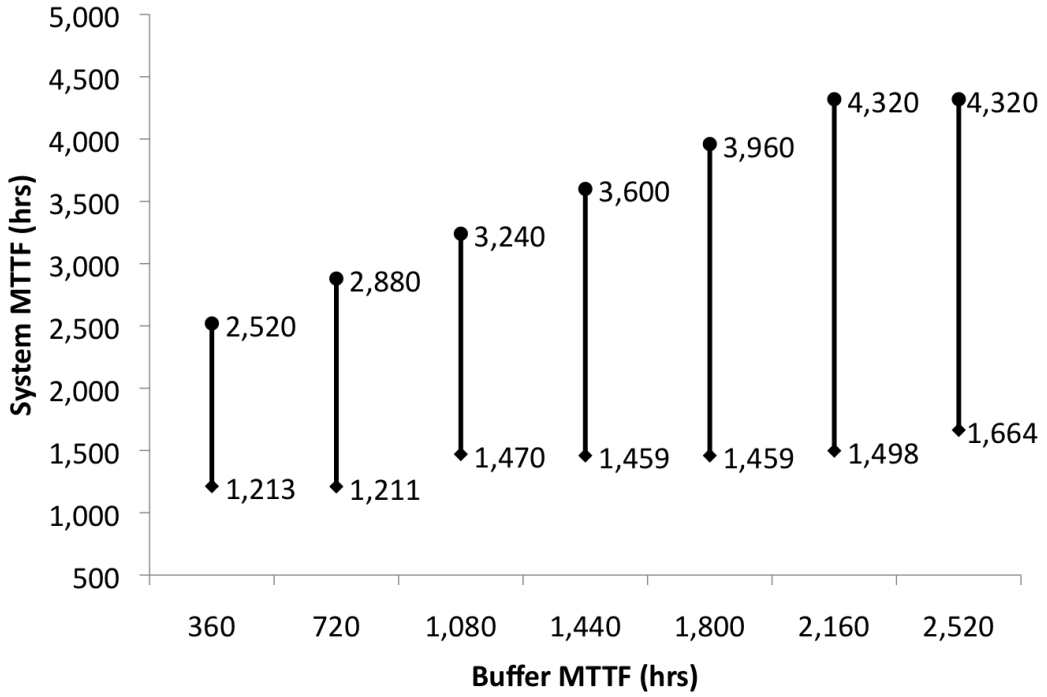


Figure 13. The impact of varying the environmental buffer volume on system reliability

D. 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 system 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 to 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 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 afforded an opportunity to better understand the impact of component impact on system performance and the adjustments necessary for improving system reliability. The model also provides critical evidence of the buffering capacity within ECLSS which allows the system to continue being functional until the buffer itself is exhausted. The current results suggest that one can define an upper bound for system reliability by utilizing the MTTF approach, however, these results may be deceptive when choosing which buffer to augment in order to maximize system reliability.

In this example a system failure is caused by the water subsystem. In Figure 14, we see the oxygen production rate suddenly drops to zero after 389 hours of operation and the system fails 48 hours later. One may initially conclude that an OGS failure must have occurred, however, Figure 15 shows that the OGS is not the cause for the system failure since the injector manages to maintain the oxygen and carbon dioxide concentrations even after the malfunction. The actual cause for the system failure is identified by looking at Figure 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. In actuality, the crew member's potable water demand could no longer be satisfied and the mission comes to an end 48 hours later.

IV. Conclusion

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

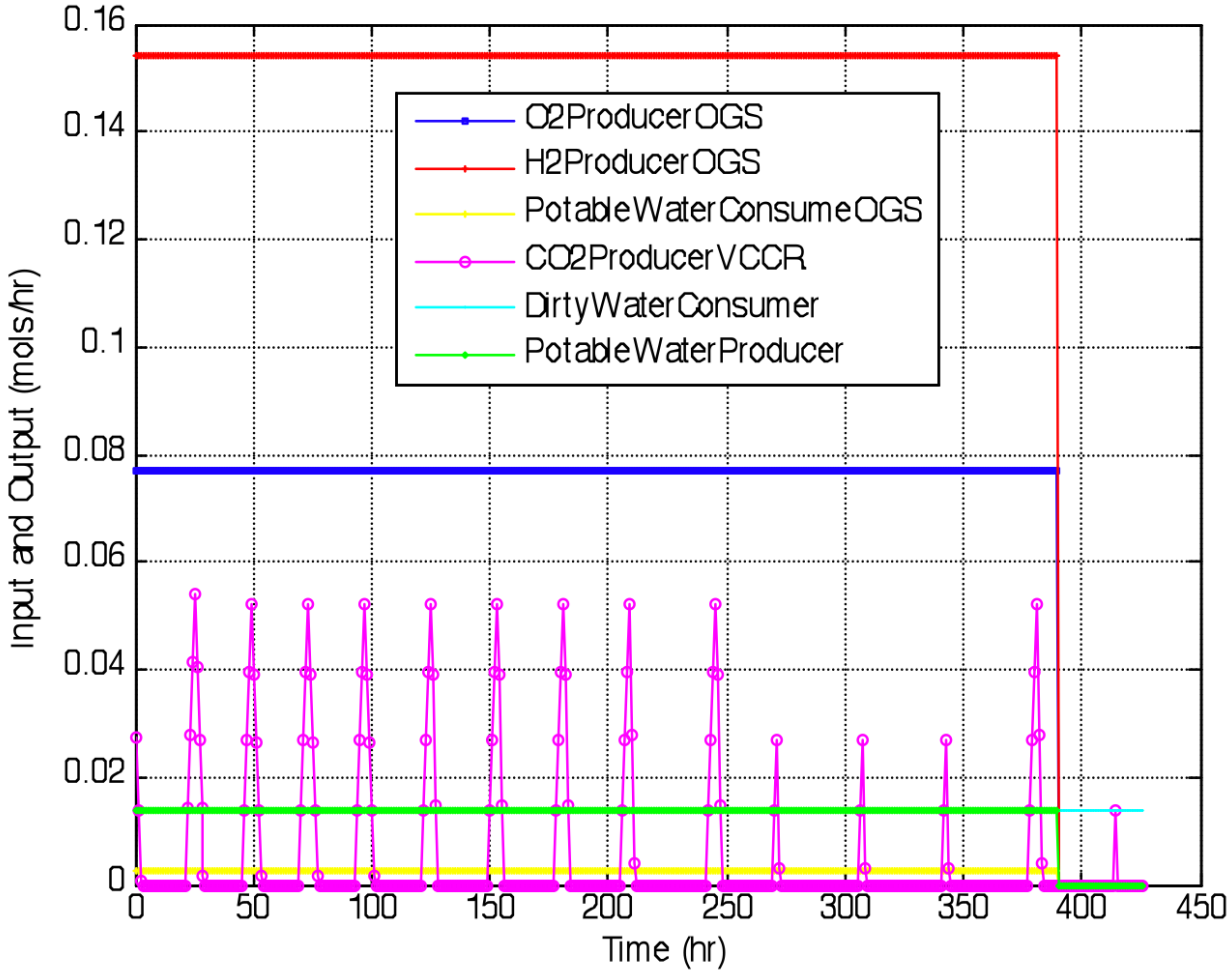


Figure 14. I/O Sensors

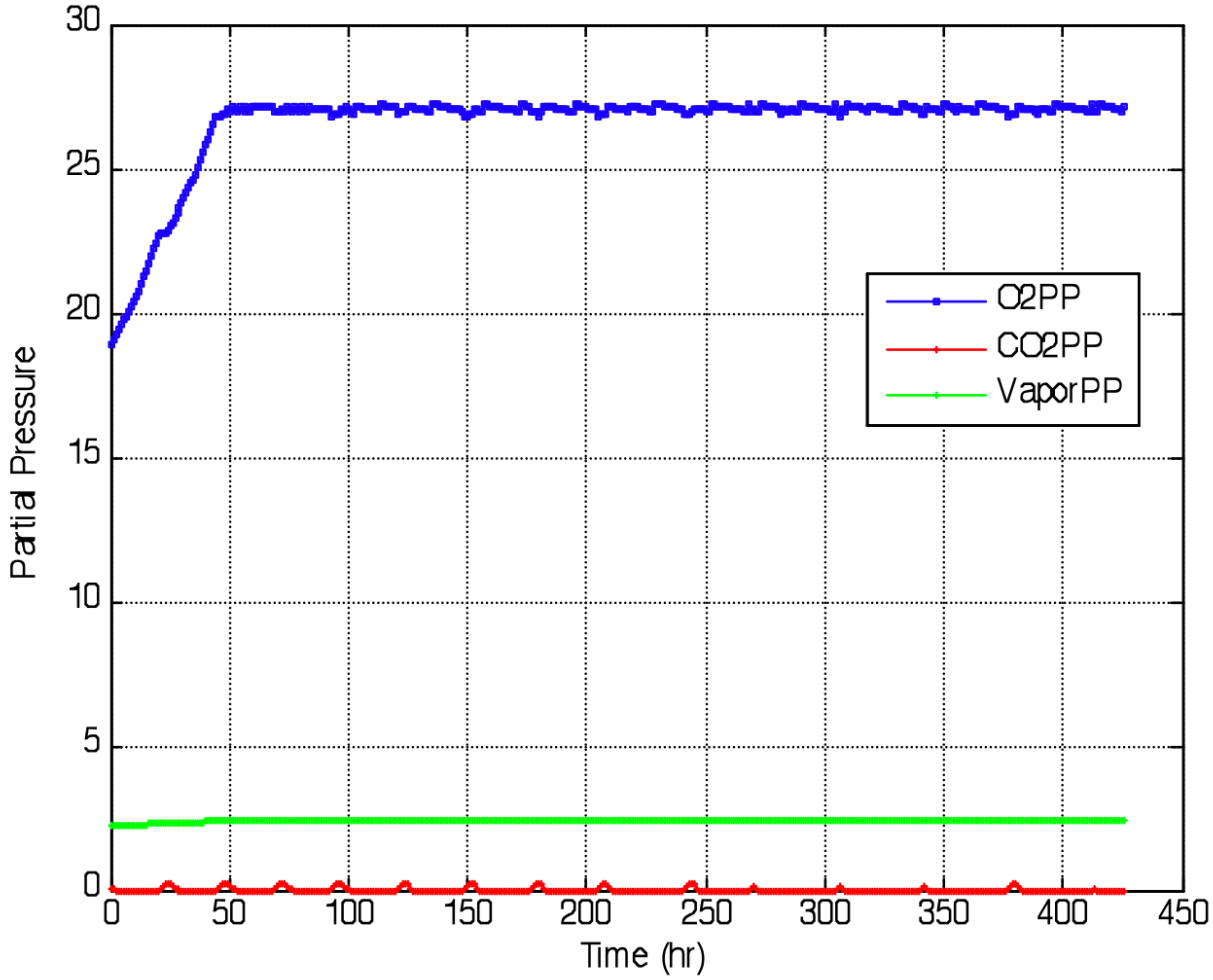


Figure 15. Environmental Condition Sensors

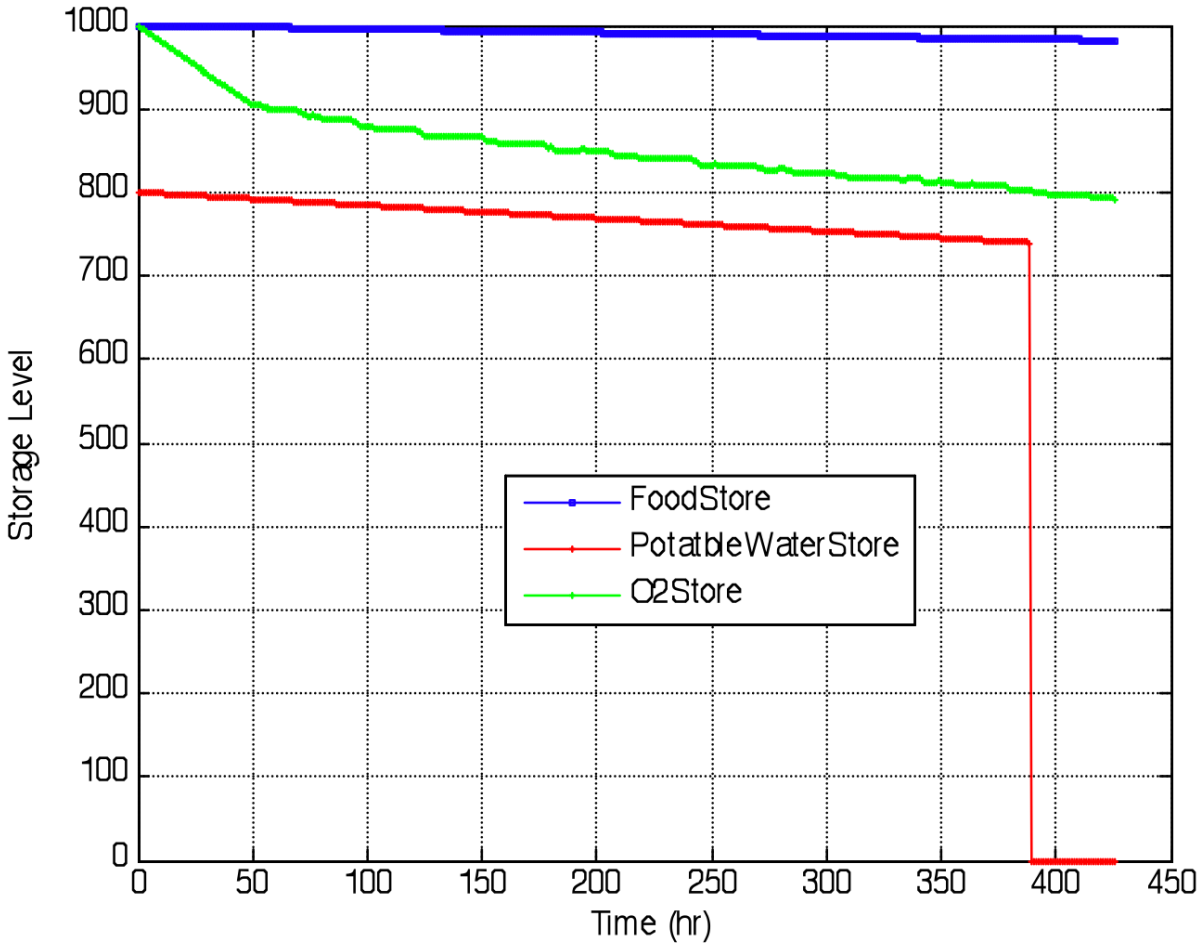


Figure 16. Store Level Sensors

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 certainly 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 impact of buffering capacity on system reliability and examples are given to illustrate how the system performs from this perspective. An approach utilizing the predicted mean time to failure of individual subsystems has been proposed here, and although it over-predicts 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.

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 under-prediction, 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 utilize the crew survival 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 unknown failures 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 also contributed to this work particularly Izaak Neveln, David Kane, and Christian Douglass who supported this work while partaking in an NSF Research Experience for Undergraduates.

References

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

[2]Leveson, N., *Safeware*, Addison-Wesley Publishing Company, Inc., 1995.

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

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

[5]Yamada, K., "Reliability Activities at Toyota Motor Company," *Reports of Statistical Application Research*, Vol. 24, 1977.

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

[7]Pagés, A. and Gondran, M., *System Reliability Evaludation & Prediction in Engineering*, Springer-Verlag, NY, 1st ed., 1986.

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

[9]Anonymous, *Guidelines for Hazard Evaluation Procedures, with Worked Examples*, Wiley-AIChE, 2nd ed., 1992.

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

[11]O'Connor, D. T., Newton, D., and Bromley, R., *Practical Reliability Engineering*, Wiley, West Sussex, England, 4th ed., 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, 2003.

[13]Rodríguez, L. F., Bell, S., and Kortenkamp, D., "The Role of Modeling in Advanced Life Support System Design and Operation," Tech. rep., 2004.

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

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

[16]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*, No. 2007-01-3027, SAE, 2007.

[17]Rodríguez, L. F., Bell, S., and Kortenkamp, D., "Use of Genetic Algorithms and Transient Models for Life Support Systems Analysis," *AIAA Journal of Spacecraft and Rockets*, Vol. 43, No. 6, 2006.

[18]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, 2004.

[19]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, 2008.

[20]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, 1996, p. 14.

[21]Horneck, G. and Comet, B., "General human health issues for Moon and Mars missions: Results from the HUMEX study," *Advanced Space Research*, Vol. 37, 2006, pp. 100–108.