# Prediction of Reliability and Cost for 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. However, system reliability requirements are subject to many constraints, particularly the mission cost. This paper presents a coupled analysis of cost and reliability for optimal exploration life support system design. Simulation tools capable of representing complex dynamical systems with configurable uncertainties are utilized for reliability prediction in comparison with the classical reliability prediction approaches.**

**The motivation of this work emerged from the understanding of the conventional reliability prediction approaches and the currently proposed life support system reliability designs for CEV, Lunar Outposts, and other long-term missions. Literature review on previous studies indicates a significant knowledge gap that needs to be addressed so as to accurately evaluate the reliability of environmental control and life support systems. Such a gap is believed to be resulted in by the unique characteristics associated with ECLSS and other environmental systems.**

**The results presented in this paper consider the difference between reliability prediction results obtained from the traditional approaches and the newly developed method which has been adjusted to address the new challenge. Meanwhile, simulation and statistical analysis results are utilized to quantify the impact of buffering capacity, contingency plans, and maintenance strategies on reliability prediction for ECLSS. A brief investigation of the system cost will also be performed to provide preliminary suggestions for balancing system reliability requirements and the associated costs.**

## I. Introduction

### A. Significance of Study

Unlike simple systems that can be accurately represented by various combinations of series or parallel reliability block diagrams, large scale complex systems used by NASA feature the nondeterministic characteristics and remain as a major challenge for precise reliability prediction.

Robust systems with multi-degree fault tolerance and well proven contingency plans are always needed by NASA and its space exploration program. Such a serious need was highlighted after the Columbia space shuttle tragedy and President Bush's declaration[1] for replacing space shuttle and returning to Moon before

*Graduate Student, Department of Agricultural and Biological Engineering, and Department of Aerospace Engineering
†Corresponding author. Tel.: (217) 333-2694; Fax: (217) 244-0323 . Email address: lfr@illinois.edu. Assistant Professor, Department of Agricultural and Biological Engineering.
‡Research Scientist, TRACLabs Inc.
§Senior Scientist ~~and Vice President,~~ TRACLabs Inc.
¶Undergraduate Student, School of Aerospace Engineering

2020. Long duration human activity in the Lunar Outpost has been proposed while further journey to Mars has been studied continuously. As mission length increases, resupplies of food, water, air and life essentials become more and more complicated and 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 design of such a robust system involves accurate reliability prediction which takes into account random component failures and their cascading effects, contingency planning and maintenance strategies, and most importantly, the buffering capacity of such a system.

Current NASA reliability analysis is a "lessons learned" style database built on historical data and expert opinions. Reliability, or failure probability, is determined by experiments, or more often, by assumptions. A widely used data base is called ISS Risk Management Application (IRMA)[2] which emerges from Futron Integrated Risk Management Application.[3] It uses a two dimensional risk assessment approach to predict "likelihood" and "consequence" of a certain event. The judgment is done 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 potential Probabilistic Risk Assessment (PRA) considering the failure modes of the Space Shuttle.[4] In this approach, failure modes are identified by any personnel working in Space Shuttle design, maintenance, operations, or analysis. Tractions of failed components are performed to evaluate their impacts on system health. Meanwhile, Failure Modes and Effects Analysis (FMEA)[5] becomes popular in the reliability industry due to its successful applications in many important projects, such as the Concorde and Airbus projects,[6] the Lunar Module LEM,[7] and many other applications, such as military systems, car manufacturing, and nuclear power plants.[8,9] Other alternative approaches exist as well, including Fault Tree Analysis (FTA),[10] What-If Analysis,[4] Functions-Components-Parameters Analysis (FCP),[11] and Hazard and Operability Method (HAZOP),[12] all coming from analogous challenges existing within the chemical processing or nuclear industry.[13,14] The limitation of these approaches can be summarized as follows,

1. All the approaches either heavily rely on operational data, or on the opinions from individuals close to the system. Inaccuracy is likely to be caused by lack of data and expert subjectivity during the process.

2. The magnitude of the efforts required to assemble all the possible failure modes limits their applicability. There's no guarantee that all the conditional probabilities will become available due to the limited ability in destructive life testing for components and the integrated system.

3. In the case that there is a large but incomplete amount of data available, the effectiveness of using these data depends on the focus and objectivity of the assessment team.

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

5. The balance between reliability and cost is not readily available for quantitative measurement and design optimization.

Overall, all these limitations reveal the concern that the classical reliability analysis approaches may not be as precise and effective for systems like life support systems. This paper will present the recent findings to answer this question.

### B. Research Objectives

The main contribution of this paper lies in demonstrating the capability of the newly developed reliability assessment approaches and the component-based simulation tool for studying the reliability and cost of complex environmental systems in space applications. The virtual environment we built is anticipated to result in the following advantages:

- Provide a virtual testing bed which allows mission designers to test different system designs and study the tradeoff between system reliability and cost;
- 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;
- Study the tradeoff between cost (crew time, redundant hardware) and various contingency plans;
- Compare system ESM (Equivalent System Mass), MTTF (Mean Time To Failure), components' MTBF (Mean Time Between 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 statistical methods qualitatively and quantitatively.

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 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 of the three-phase plan has been completed and the corresponding results are presented in this paper. The rest 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 experiment results obtained for this system; Section IV presents the conclusions and the directions for future research.

## II. Methodology

### A. Reliability Modeling and Prediction Approaches

Three reliability prediction methods will be described in this section, including RBD (Reliability Block Diagram), MRBD (Modified Reliability Block Diagram), and MC (Monte Carlo) style simulation with MLE (Maximum Likelihood Estimation). The reasons for selecting those methods will also be explained in this section.

#### *1. Reliability Block Diagrams*

A fundamental approach to represent system reliability in terms of component reliability is Reliability Block Diagram (RBD).[15] 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.*

In conventional reliability theory, the integrated system is in its operational state when there is an open pathway between the beginning and ending points presenting the inputs and outputs of the system; the system is determined to be in a failed state when all the paths between these two points are broken. The advantage

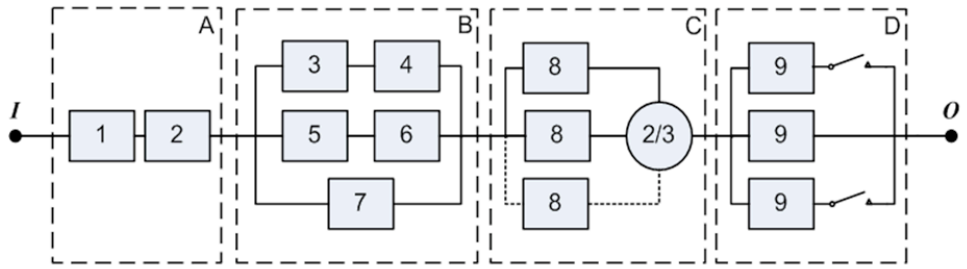



**Figure 1. Reliability Block Diagrams**

of such a graphical representation of system configuration is that the reliability can be determined using a binary characterization of the state for each component within the system, for example, $x_i$, $i = 1, \ldots, n$. A time-variant probability function $R(t)$, which equals one if the system is in a working state (UP), and zero if the system is in a failed state (DOWN), is known as the reliability function of the system with respect to time. And $F(t) = 1 - R(t)$ is referred to as the failure function. Mathematically, the reliability function of a series system can be expressed as,

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

And 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 more commonly used in practice 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,

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

In all cases, it is assumed that each component fails independently and all the components are identical.

Another type of redundancy is called passive (offline) redundancy. In this case, a two-unit system functions successfully when the primary unit does not fail, or if the primary unit fails during the operating time t and the 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 $\tau$, $0 < \tau < t$, and the standby unit functions successfully from $\tau$ to time t. In other words, the reliability function the system becomes,

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

where $R_1(t), R_2(t)$ denote the reliabilities of the primary unit and the standby unit at time t respectively, and $f_1(t)$ = the p.d.f. of the failure time distribution of the first unit.

More generally, we can extend the two-unit standby system to n-unit a standby system. The reliability of the multiunit standby system is given by

$$R(t) = e^{-\lambda t}(1 + \lambda t) + \frac{(\lambda t)^2}{2!} + \cdots + \frac{(\lambda t)^{n-1}}{(n-1)!} \tag{5}$$

The difference in 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. 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 level. 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, or independent component failures need to be assumed. Secondly, the components in the system needs 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 needs to be assumed that no preventive or corrective maintenance is available for system components since maintenance actions will drastically change the fundamental implementation of RBD and add significantly amount of complexity to the problem. However, contingency plans are still being tested, for example, online redundancy can be modeled using parallel structures consisted of identical or non-identical components while offline redundancy can be modeled using switches.

### 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 conditions, rather, crew condition is of the major concern for mission successful. The major innovation presented here is the use of a reliability block to represent the system buffering capacity which supports crew habitation after certain regenerative component has failed. A graphical representation of the modified system reliability diagram is depicted in Figure 2 where the dashed line circles the buffers of the system.

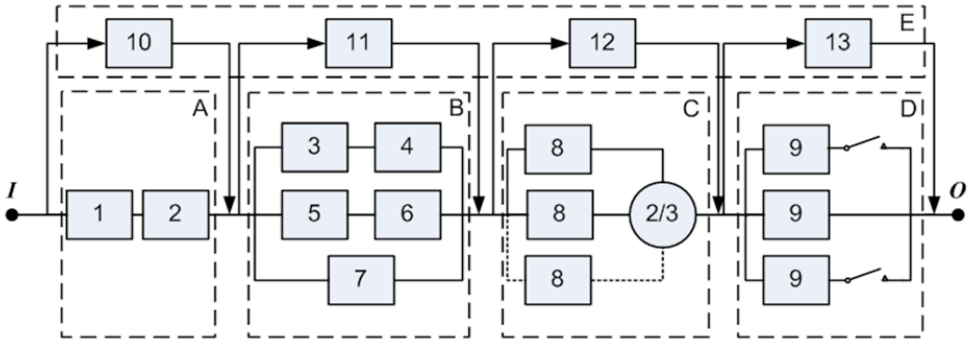



**Figure 2. Modified Reliability Block Diagrams**

The system E in the figure represents the buffering capacity, or more generally, the resources within 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 provide the necessary resources to keep the crew members alive when certain regenerative system A, B, C or D fails to be functional. This modification is system reliability diagram is built to affect the 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 parallel configuration. However, the remaining challenge which is to select a function that physically represents the buffering capacity is hard 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 halted due to component failure. Moreover, the authors have also considered repairable components, in which case, the buffering capacity should also be self-restorable, meaning that the habitation environment can regain the lost resources once the failed component becomes functional again. The rate of recovery is essentially the difference between production rate and consumption rate, and the buffering capacity needs to be properly sized and not to exceed the total capacity of the habitation environment.

A normal reliability model has been proposed to represent the buffering capacity, the shape of the model is shown in Figure 3. The advantage of a normal model is that it can mathematically simulate the process of switching on and off using approximately binary states, It can also 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:

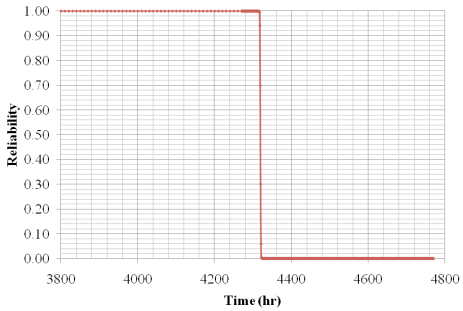



**Figure 3. A normal reliability function with $\mu = 4320, \sigma = 1$.**

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

where $\mu$ and $\sigma$ are the mean and the standard deviation of the distribution. The plot in Figure 3 has a very sharp reliability decrement after 4320 hours since ($\mu$) and $\sigma$ are selected to be 4320 and 1 respectively. These values need to be selected by the system analyst for properly sizing the buffering capacity for real systems.

### *3. Simulation and Statistical Methods*

Simulation Tool BioSim is a dynamic system simulation tool developed by NASA Johnson Space Center over the past few years.[16–19] Mathematically models for typical components found in various life support systems are fully integrated with the simulation infrastructure to achieve accurate simulations of realistic life support systems. Real-time simulation progresses in hourly increments, with each unit process producing and consuming various resources to and from the designated stores. An XML configuration file containing the design of the system initializes the simulation. Additional functionality can be developed and added to the component models via the XML configuration file, such as random failure and stochastic performance.[20] BioSim has been successfully utilized and verified in many ECLSS optimal design applications, including reliability analysis, control system testing, and power system design verification.

Monte Carlo Simulation MC[21] simulation 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. For example, different maintenance schedules and quality, reliability degradation, repair priorities, and the focus of this paper, buffering capacity. In this study, 5 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 and system design improvement purposes. For such an experiment design, MC simulation seems to be the only viable approach to fully study complex systems operated under realistic logistic strategies even though the approach is known to have disadvantages such as computationally intensive and notably expensive in post simulation data analysis. In our application, the major concern is that even if a numerous amount of 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 Method MLE 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

$$L(X_1, \ldots, X_n; \Theta) = \sum_{i=0}^{n} f(X_i; \Theta) \qquad (7)$$

The maximum likelihood estimator (MLE) of $\Theta$ is that value $\Theta$ that maximizes $L$. In most cases, the MLE is obtained by letting the differentiation equation to be zero and solving for the unknowns.

For numerical simplicity, we illustrate the procedure by utilizing MLE for deriving the parameter for the exponential distribution. Assuming a sample of size $n$ from the distribution, the likelihood function is

$$L(x_1, \ldots, x_n) = \sum_{i=0}^{n} \lambda e^{-\lambda x_i} = \lambda^n e^{-\lambda \sum_{i=0}^{n} x_i} \qquad (8)$$

so that $\log L$ becomes

$$logL = nlog(\lambda) - \lambda \sum_{i=0}^{n} x_i \tag{9}$$

Differentiation with respect to $\lambda$ leads to the likelihood equation

$$\frac{n}{\lambda^*} - \sum_{i=0}^{n} x_i = 0 \tag{10}$$

with solution

$$\lambda^* = \frac{n}{\sum_{i=0}^{n} x_i} = \frac{1}{\bar{x}} \tag{11}$$

where $x_i$ is the time of the $i$th failure and the MTTF is simply the inverse of $\lambda^*$

The same approach can be applied to many other widely used reliability models, such as Two-Parameter Exponential distribution model, Weibull distribution model, Normal and Lognormal distribution model, Inverse Gaussian distribution model, and so on. The final selection of system reliability model needs to be made so as to best match the actual experiment results.

### B. Cost Assessment

To completely measure the quality of a life support system, we need to investigate both its reliability and the associated costs. The proxy for cost measurement in space applications is called Equivalent System Mass, or ESM. It is a conversion metrics in which system design aspects are converted into mass in the unit of kilograms. A Java-based ESM calculator has been developed and integrated with the BioSim tool to evaluate the costs of various system configurations selected for reliability improvement. It is capable of retrieving information from the XML configuration files used by BioSim and compute the ESM values for subsystem and the integrated system.

For verification purpose, another viable tool that NASA is currently using called *Advance Life Support Sizing Analysis Tool*, also known as ALSSAT, is also utilized. It is a robust spreadsheet based program that has many inputs for the various aspects of life support system design and configuration. Due to the complications of integrating XML with visual basic and Microsoft Excel, a new ESM calculator is written in JAVA to take advantage of the application programming interfaces (APIs) previously established in BioSim. In this practice, the integrated system is divided into five subsystems, including air, food, thermal (power), waste, and water. Each of the unit process existing in the XML configuration file is distinctly associated with one of the five categories. The ESM values are thus calculated for each subsystem in terms of mass, volume, power, cooling, and crew time. The weighted summation of these values is essentially the ESM of the integrated system where the conversion factors are chosen according to the values specified in the Baseline Values and Assumptions Document (BVAD)[22] and the ALSSAT tool for various mission scenarios, such as Lunar transit, Lunar surface, Mars transit, and Mars surface. To allow end user input necessary parameters for the ESM calculator, a graphical user interface is also designed. It further simplifies the ESM calculation process and provides a quick read out of the returned ESM values.

## III. Case Study

The case study presented in the paper carries the objectives of:

1. Develop a system for which various reliability modeling and prediction approaches can be performed and compared;

2. Predict the reliability function of the integrated system 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

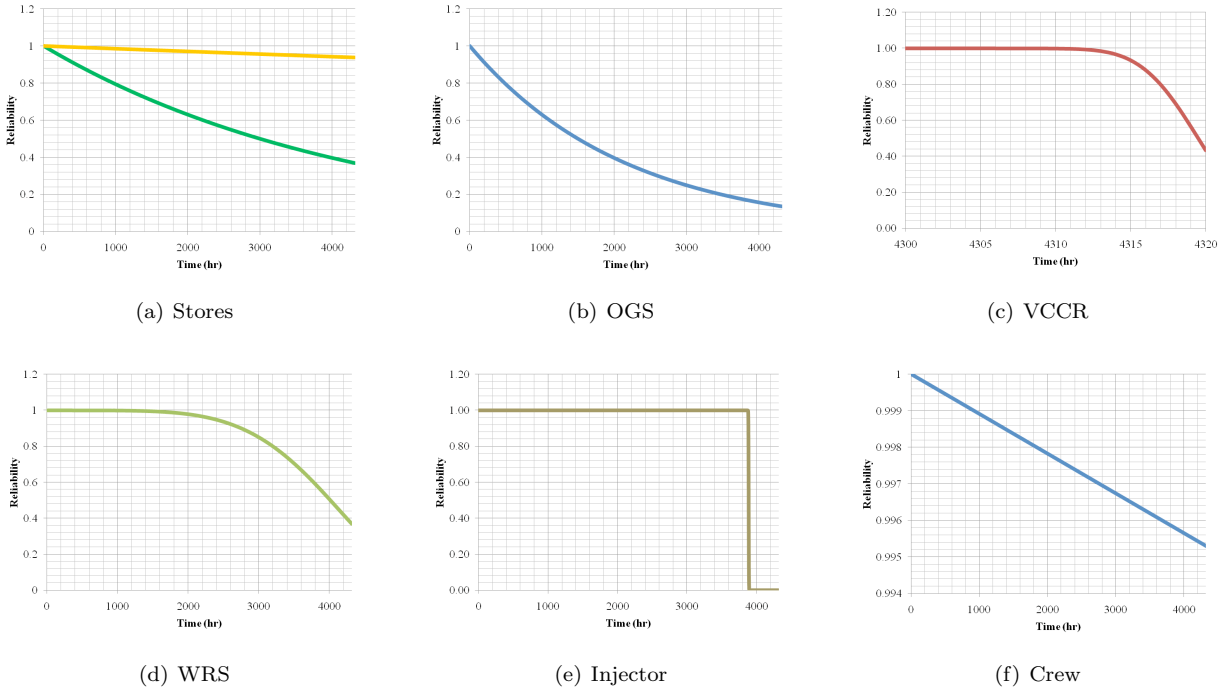
The ECLSS tested in this study is ~~designed~~ a six-month Lunar Outpost mission. It is consisted of four types of components: *storage components* (gas stores, water stores, and other resources stores), *regenerative components* (Oxygen Generation System, Water Recovery System, and Variable Configuration $CO_2$ Removal System), *control components*(Air Injector and Actuator), *crew member* (one crew person with moderate activity schedule).

Some system level assumptions are designed and applied to all reliability prediction approaches, including:

1. Components in the system only have two states, UP and DOWN. Performance degradation is not currently under consideration.
2. The habitation environment can provide enough resources for the crew member to survive for 30 days, which means the $\mu$ value for the normal model representing the buffering capacity is selected to be 720.
3. Component failure is assumed to be independent, however, in simulation, OGS, VCCR and WRS cannot produce resources if the power supply has been discontinued. Note that those systems are still functional which will later allow us to test parallel system with multiple resources stores.
4. All components are non-repairable and no preventive maintenance is provided.
5. System failure is determined by component reliability function in RBD and MRBD, while for simulation, it is determined by crew survival conditions.

### B. Assumptions for Component Reliability

Before assigning realistic reliability models to each of the component within the system, a preliminary experiment is conducted using the assumption that all the components are subject to exponential reliability model. Such a tested is considered to be necessary due to the fact that exponential reliability model is mathematically friendly for reliability analysis. The only parameter for exponential model is $\lambda$ whose inverse has the physical meaning of MTTF. The same MTTF values are later utilized for more realistic assumptions. The following section describes the assumptions made for system components and the component reliability functions are graphically represented in Figure 4.




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

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

**Figure 4. Assumptions for component reliability.**

### 1. *Storage Component Reliability*

Gas stores and water stores use the same reliability model since those tanks are very similar in function and considerably reliable. Exponential reliability model is assigned to the storage components with a MTTF value of 8 years which has been tuned for reliability comparison purpose. The assumptions are made such that the hazard rates[a] of the storage components remain as constants throughout the entire mission.

Resources stores for food, power and water also use exponential models but with different parameters. 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 storage condition change. Power store is also more likely to fail than the other storage components since it needs to face many failure modes, for example, short circuit, overload, overheat, or black out periods. Table 1 summarizes the design parameters for each of the storage components within the system.

**Table 1. Storage component reliability assumptions.**

| Component | Model | $\lambda$ | 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*

More realistic reliability assumptions were made for the regenerative components. The OGS is considered to be the most unreliable component within the system boundary since there were three reported OGS[b] failures on ISS, occurred on September 8, 2004, January 1, 2005 and September 18, 2006 respectively during the eight-year mission.[23] For the purpose of demonstrating the impact of component random failure on system reliability, exponential model is selected for OGS with a down-scaled MTTF which is one-third of the mission length. Another important regenerative component, 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 data and current test data[24] 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 WRS to exhibit the hazard rate variation over time. VCCR, on the other hand, is much more reliable. A normal model is assumed for 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 | $\lambda$ | $\mu$ | $\sigma$ | $\beta$ | MTTF |
|---|---|---|---|---|---|---|
| OGS | Exponential | 0.00046 | – | – | – | 2160 hrs |
| WRS | Weibull 2 | 0.00023 | – | – | 3 | 4320 hrs |
| VCCR | Normal | – | 4320 | 5 | – | 4320 hrs |

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

[b]The Russian unit, Elektron

### 3. *Control Components*

The injector in the system is designed to consume $O_2$ from the storage tank and inject it into the habitation environment so as to adjust $O_2$ and $CO_2$ partial pressure. It has to experience repeated cyclic loads and therefore, a MTTF value that is 90% of the mission length is assigned to a Normal model to describe its reliability over time. The actuator utilized here is a passive component for control purpose in the simulation tool. Since it has no direct impact on system reliability, its reliability function is not specified. Table 3 shows the parameters selected for the reliability function of the control components.

**Table 3. Control component reliability assumptions.**

| Components | Model | $\mu$ | $\sigma$ | MTTF |
|---|---|---|---|---|
| Injector | Normal | 3888 | 3 | 3888 hrs |

### 4. *Crew Members*

Crew member is consider to be very reliable although they are still subject to failures such as severe injure and illness. According to the crew reliability study conducted by Horneck and Comet,[25] we designed a linearly decreasing reliability function for the crew member 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 | $-1.09 \times 10^{-6}$ |

## C. Reliability Prediction

### 1. *Reliability Block Diagrams*

As is previously described, the system reliability has been predicted using the proposed reliability prediction approaches. The RBD approach, the 'naive' approach since it does not take system buffering capacity into account, is first tested by numerical derivation and stochastic simulation, utilizing Excel and Matlab respectively. Such a self-validation process is designed to provide confidence for more complicated experiments where Matlab simulation approach becomes the only viable approach for reliability prediction. System reliability over time is first computed in Excel utilizing component reliability which known for the entire mission while the Matlab simulations are conducted using a failure decider which determines component failure status at any given time and then collect the system failure data for the MLE process which returns the estimated parameters for the selected system reliability model. Figure 5 illustrates the simplified system whose components are simply connected in series and will cause system failure if any single of them fails. Such a simplification is considered to be valid based on the fact that it satisfies the basic requirements of modeling a typical life support system which is consisted of an air subsystem, a water subsystem, several resources stores, and crew members. However, such a simplification is intuitively inaccurate for ECLSS analysts since the actual system will not fail instantly due to a unit process failure; on the contrary, it can survive until all the resources in the habitation environment are exhausted by the crew members. Therefore, it is expected that an underestimation of system reliability will be observed in the experiment. The reliability prediction results are presented in Figure 6 which illustrates the reliability prediction results for several different scenarios designed for the RBDs approach. It can be observed that the RBD approach using an exponential model for all components perform the worst in comparison with 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 noticeable that the reliability prediction results obtained from Excel calculation and Matlab simulation match perfectly with each other. This result is consistent with our expectation and it adds credibility to the failure decider we implemented for destructive life testing experiments. Lastly, it needs to be mentioned that the system reliability becomes

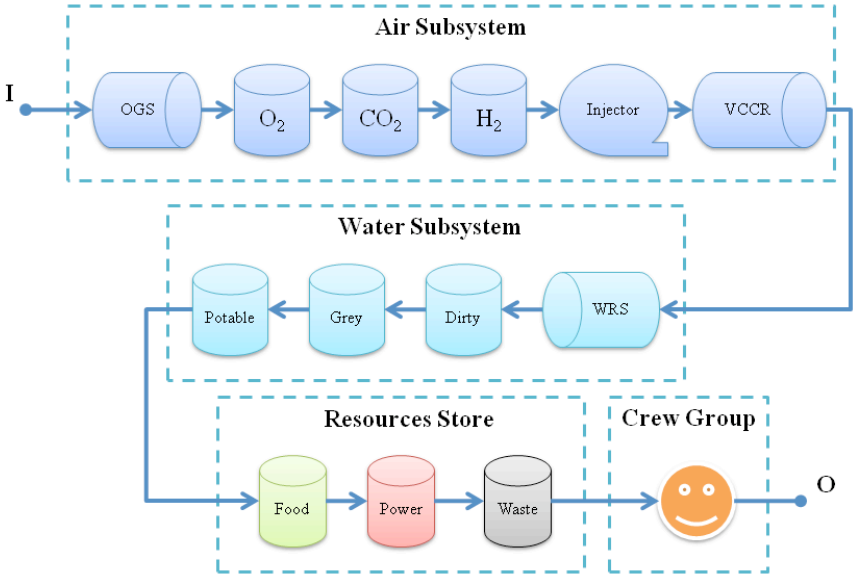



**Figure 5. Reliability block diagram for ECLSS without buffering capacity.**

rather low at the end of the mission. This is due to the fact that the more complex a series becomes, the less the system reliability is. Such a disadvantage of RBD raises the question that if there is a way to improve RBD so that it can become applicable for more complicated reliability analysis.

### *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 naive system representation. The major difference is the introduction of buffers for each regenerative subsystem, or the entire system, as is illustrated in Figure 7 and Figure 8 respectively.

The reliability prediction results for both scenarios are obtained using Matlab simulations since various reliability models in a parallel-series configuration make the system reliability function too difficult to derive mathematically. The same failure decider, as is previously described, is utilized for simulating component random failure.[20] System failure time is recorded for 100 identical systems stochastically. Those data are analyzed using MLE to determine the parameter for the exponential model which is capable of predicting system reliability and comparable with the results from the naive series system tested using RBDs. The results presented in Figure 9 demonstrate the difference between RBD and MRBD in reliability prediction. The results from MRBD approach is 3.7 times higher than those from RBD in average. It is also noticed that the one buffer system performs 30% worse than the system with several buffers, although their 95% confidence interval illustrated using the dashed lines overlap with each other at the early stage of the life cycle.

### *3. Simulation and Statistical Methods*

The simulation tool, BioSim, is utilized to perform destructive life testing and generate system failure data. These data are thus processed using MLE to assess the parameters for the exponential model that describes the system reliability. Figure 10 depicts the mass flow of the simulated system. Several additional assumptions are made for the simulation, including:

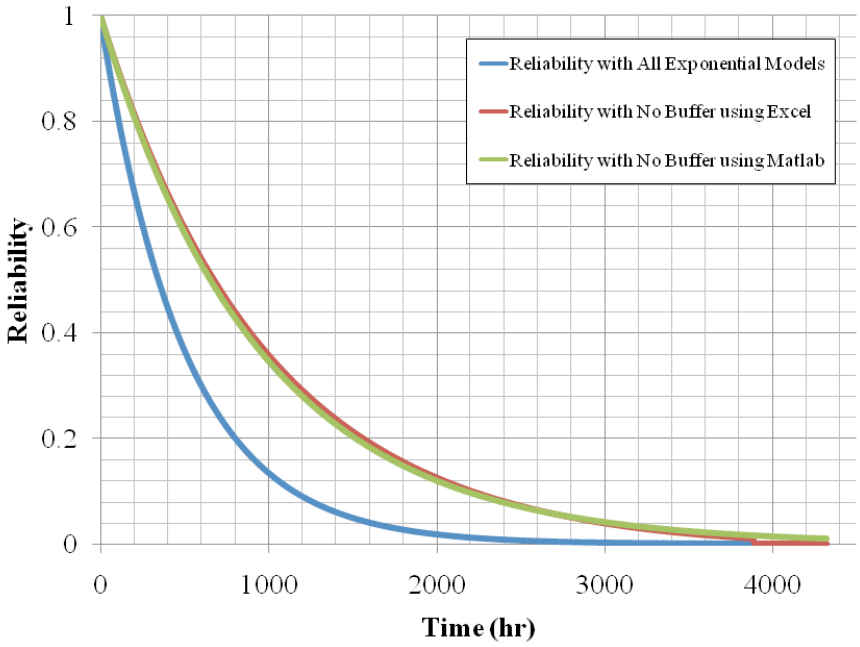



**Figure 6. Reliability prediction results from the RBD approach.**

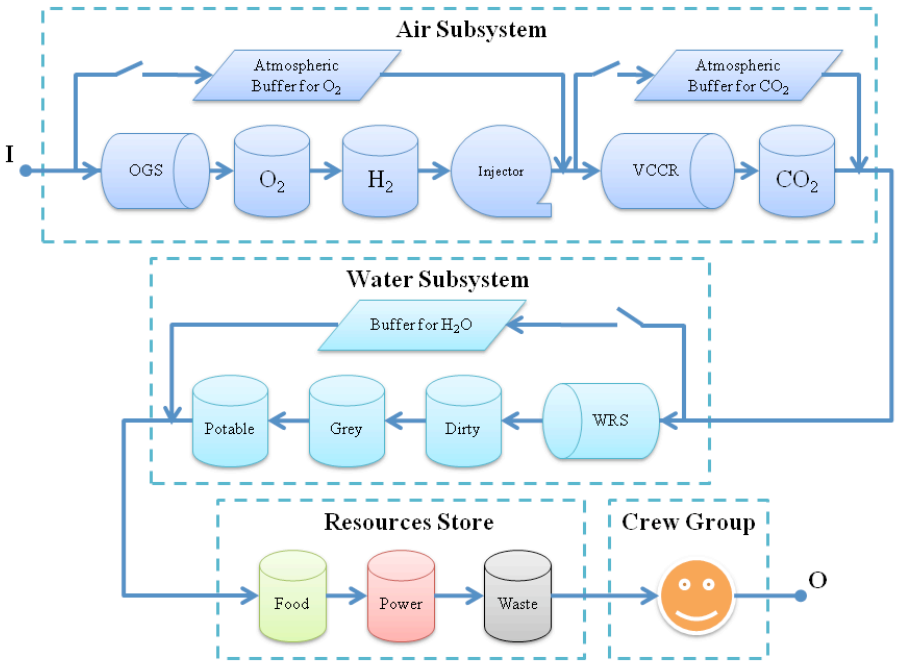



**Figure 7. Modified reliability block diagram for ECLSS with several buffers.**

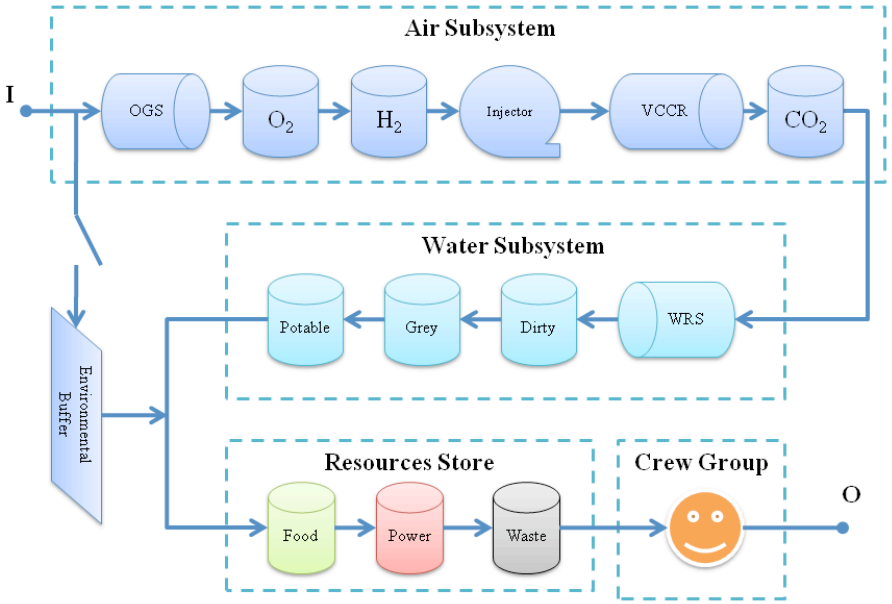



**Figure 8. Modified reliability block diagram for ECLSS with one buffer.**

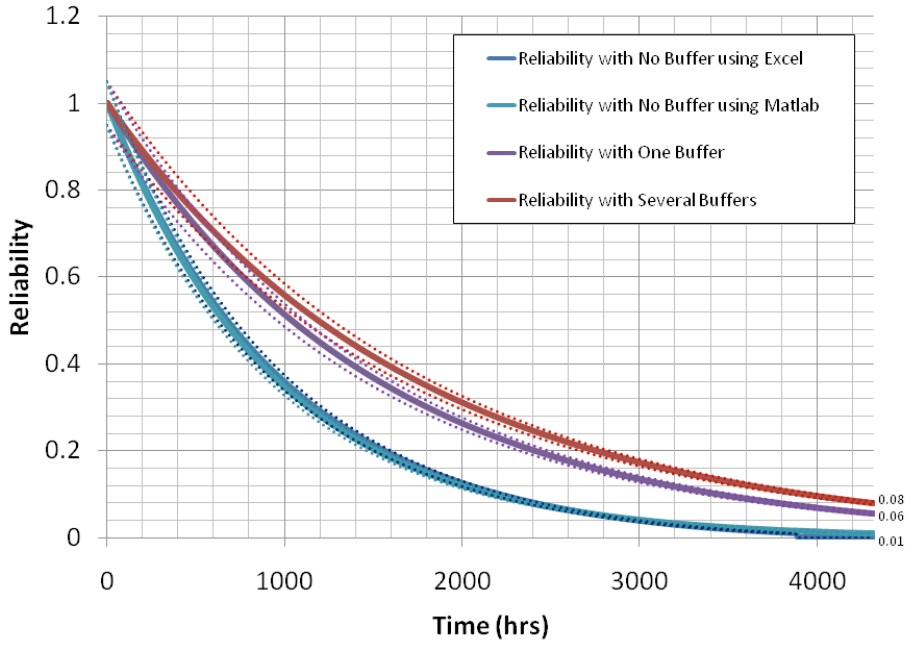



**Figure 9. Reliability prediction results from the RBD and MRBD approaches.**

1. OGS, VCCR, and WRS require power supply, which means if the power store is in a *DOWN* status, all the regenerative component will not be able to consume and produce any resources even if they are still functional.

2. For all storage components, if the amount of resources have exceeded the designed capacities, the extra amount 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 regenerative components are not functioning at their full capacity. More crew members can be added with additional power supply so as to achieve true close-loop.

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

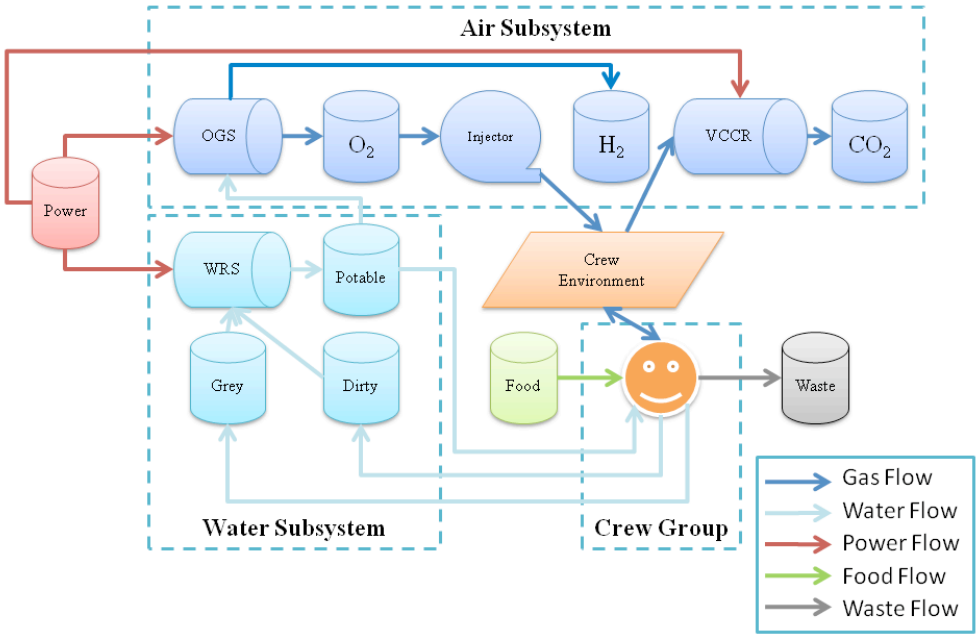



**Figure 10. Mass flow diagram in BioSim simulation tool.**

In this experiment, results are generated only using the BioSim simulation tool since no other tool readily available is capable of handling such a task. 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 $O_2$, $CO_2$ concentration. The crew is assumed to be capable of living without food for 3 weeks and without water for 2 days. The $O_2$ concentration limit takes into account both the upper bound which increases fire risk and the lower bound which causes insufficient $O_2$ for crew to breath. The $CO_2$ concentration concerns more about carbon dioxide toxicity. Two illustrative example of system failure modes are discussed in the following section titled "*System Failure Modes*".

The reliability prediction results shown in Figure 11 exhibit that the average reliability prediction results obtained using the simulation tool is approximately 27 times higher than the ones from RBD and 4 times better than those from MRBD. It is obvious that the simulation approximates system dynamics most accurately, and therefore, the difference in reliability prediction results consolidated the concerns raised at

the beginning of the paper. These results clearly demonstrate that both RBD and MRBD approaches have limited ability in modeling and predicting reliability for complex systems and they tend to underestimate reliability for systems with buffering capacity.

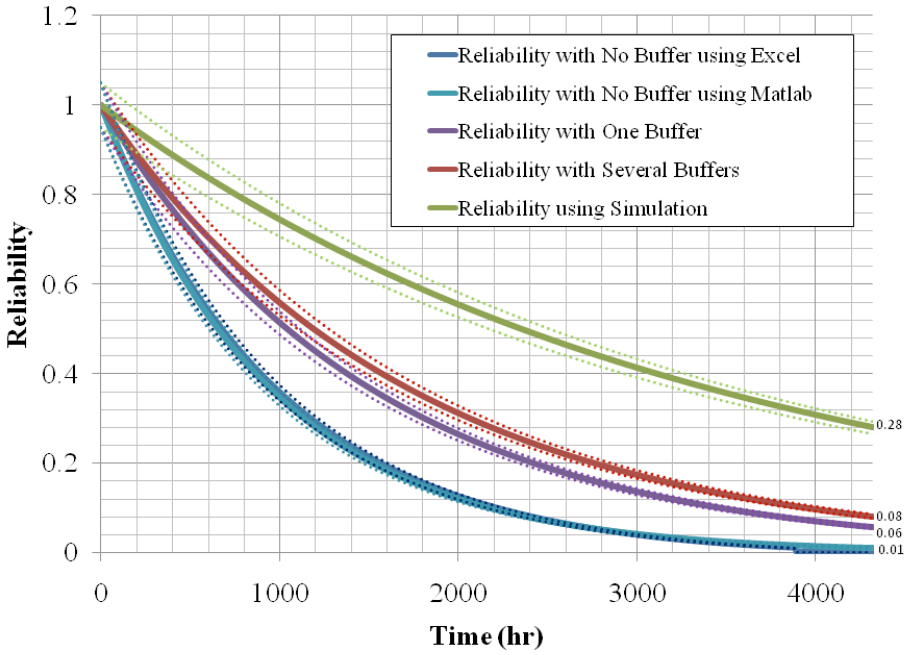



**Figure 11. Reliability prediction results from the RBD, MRBD, and simulation approach.**

### D. Cost Analysis

The ESM calculation tool has been tested using the XML files developed for various life support systems with different contingency plans. The comparison between our ESM calculator and the ALSSAT tool demonstrates the viability although some limitation has also been identified. The major advantages of the ESM calculator are: 1) Easy to use in comparison with ALSSAT; 2) Capable of directly converting XML information to ESM values; 3) Seamlessly integrated with BioSim and adaptable for other applications; 4) Accurate ESM increase/decrease trends in response to changes in mission length or type, and crew group size. The major disadvantages of the ESM calculator have also been identified, including, 1) Incapable of accurate ESM assessment for waste and thermal subsystem due to incomplete modeling of the related unit processes; 2) Lack of consideration for subsystems with multiple technology options; 3) It tends to underestimate the ESM of the overall system by 20% in comparison with the ALSSAT tool for various mission lengths and crew group sizes. A more detailed description of cost variation in response to system configurational changes for reliability improvement is planned to be discussed in a later publication.

### E. System Failure Modes

A wide range of failure modes have been considered for the ECLSS under investigation. The most frequently observed failure is air subsystem failure, usually the $CO_2$ concentration goes over the limit and terminates the simulation. Failures in food and water system have also been observed. Two system failure events are presented in this section to demonstrate how system failure can occur in the BioSim simulation tool. Figure 12 to 17 are the plots of the sensor data collected during the simulations. Those data describe the inputs and outputs of the regenerative components, the storage levels of various resources, and the environmental conditions for crew habitation. These observations can help system designers to better understand the impact of component reliability and the adjustments needed for improving system reliability. In addition, it

also provides critical evidence to further prove the existence of the buffering capacity within ECLSS which allows the system to continue being functional until the buffer itself gets exhausted.

### 1. *Water Subsystem Failure*

The first example shows a system failure caused by the water subsystem. It is observed in Figure 12 that $O_2$ production rate suddenly drops to zero after 389 hours of operation and the system fails 48 hours later. However, we know from Figure 13 that OGS is not the cause for system failure since the injector manages to maintain the $O_2/CO_2$ concentration level even at the time when the system fails. The actual cause for the system failure is identified by looking at Figure 14 where the potable water storage level drops to zero due to a failure in the potable water store. The assumption for component random failure in BioSim is that any component in a failed status will have zero input and output, and for stores, their level will become zero instantly. Therefore, since there's no potable water available for OGS to produce $O_2$, the OGS production rates become zero. More importantly, since the crew member's potable water demand can no longer be satisfied, according to the crew survivability assumptions, the mission comes to an end 48 hours later after the potable water store has failed.

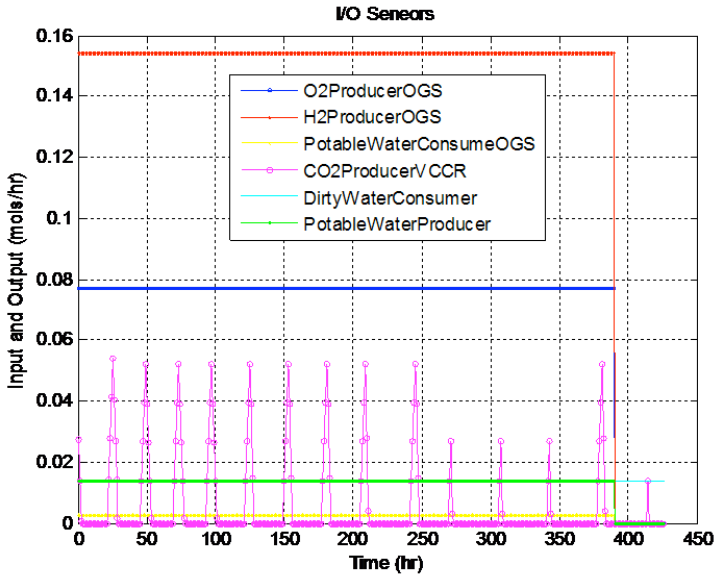



**Figure 12. I/O Sensors**

### 2. *Air Subsystem Failure*

A more frequently observed system failure is due to air subsystem failure. In this case, $O_2$ partial pressure and $CO_2$ partial pressure are the major concerns for system health. The I/O sensors capture the failure of OGS whose $O_2$ and $H_2$ production rates become zero after 1771 hours as is shown in Figure 15. It also shows that the VCCR makes a great effort to remove $CO_2$ from the system as $O_2$ partial pressure decreases and $CO_2$ partial pressure increases. We can learn from Figure 16 that the mission failed due to $CO_2$ toxication which is essentially caused by lack of $O_2$. However, the OGS failure at the early stage of the mission, is not the direct cause that terminates the simulation. After a careful observation of Figure 17, we notice that the $O_2$ storage level stops decreasing after 3503 hours. This is because the injector has failed so that it neither consumes $O_2$ from the store nor injects $O_2$ into the habitation environment. Therefore, the lesson learned here is that as long as the initial resource storage is appropriately sized, regenerative component failure will

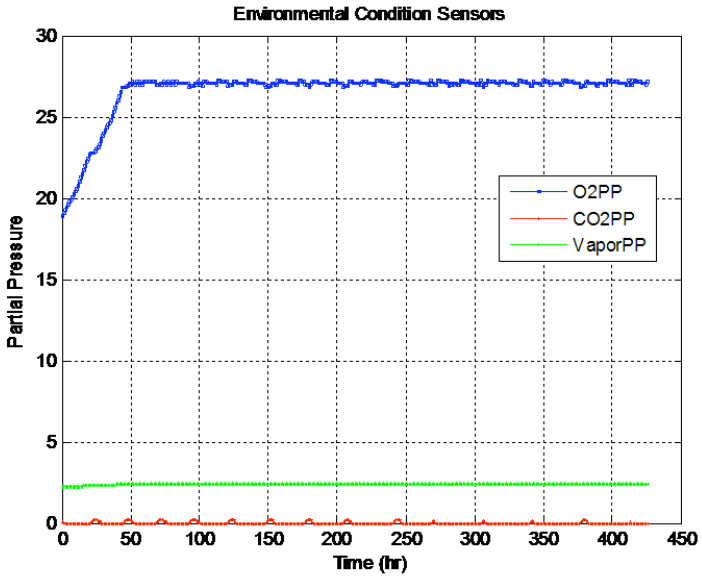



**Figure 13. Environmental Condition Sensors**

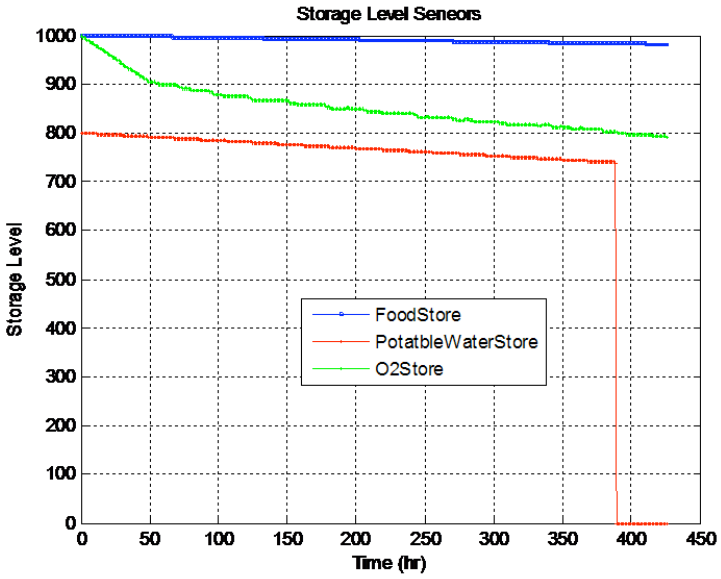



**Figure 14. Store Level Sensors**

not cause system failure instantly. However, the component that actually utilize those resources and control the system environmental conditions are more vulnerable to failures since they have direct impact on system health. For the purpose of reducing system cost and improve reliability, such type of components may should be given higher priority for owning backup units so that the system can really take advantage of its buffering capacity when individual component failures occur.

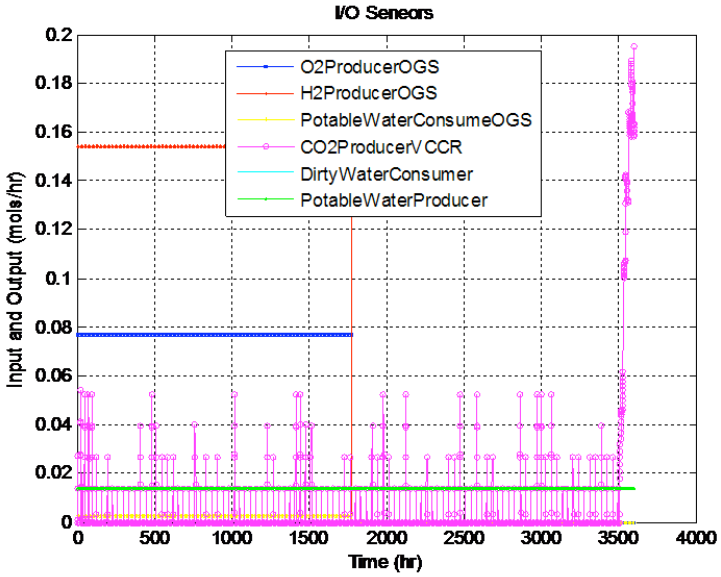



**Figure 15. I/O Sensors**

## IV. Conclusion and Future Work

This paper demonstrates the use of several reliability prediction approaches for studying the reliability of ECLSS in long term space missions. The comparison between the prediction results shows a significant difference which is believed to be caused by the unique characteristics of the system. Experiments are designed to show the impact of buffering capacity on system reliability and examples are given to illustrate how the system works with such a special quality. A high[illegible]tegrated simulation infrastructure has been further developed for reliability testing purposes, in additio[illegible]t assessment tool has also been implemented and test to provide easy access to system cost measurements. Such a combination of tools enable a long term research plan which intends to address many reliability and cost related issues, such as optimization for maintenance strategy and contingency planning. The quantification of the difference in reliability prediction results using RBD, MRBD, and the simulation approach provides an insight to the fact that some of the conventional reliability analysis approaches are no longer directly applicable for ECLSS alike systems. More research work will be needed to improve the performance of MRBD which might become a viable generic tool for studying reliability of system with buffering capacity. In addition, many new features need to be added to the current simulation tool for it to become capable of studying a even more realistic ECLSS. For instance, the preventive and corrective maintenance functions are yet to be integrated and validated. More research opportunities have been identified in this area. Firstly, more complicated system configurations, such as series-parallel, should be tested with different contingency plans to quantify the deviation in reliability and cost. Secondly, the efficiency of the simulation tool needs to be improved so that a larger scale Monte Carlo simulation can be executed to cover the search space more comprehensively. Lastly, artificial intelligent search algorithms need to be tested for achieving design optimization objectives at a reasonably low cost.

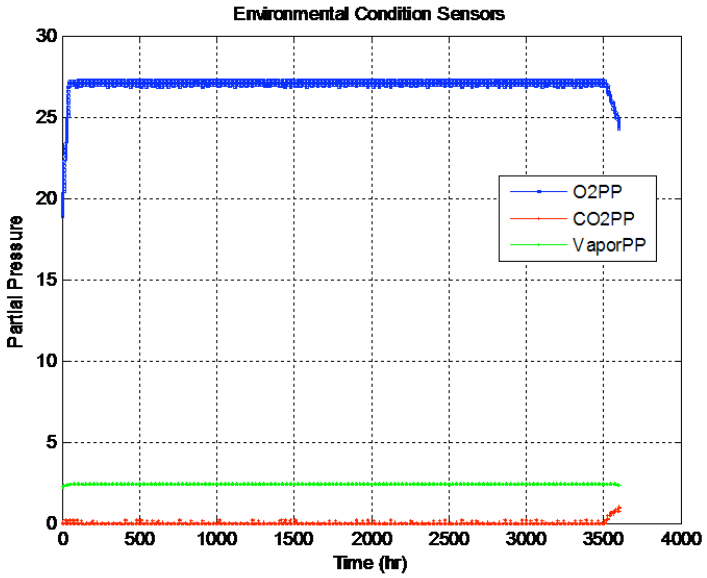



**Figure 16. Environmental Condition Sensors**

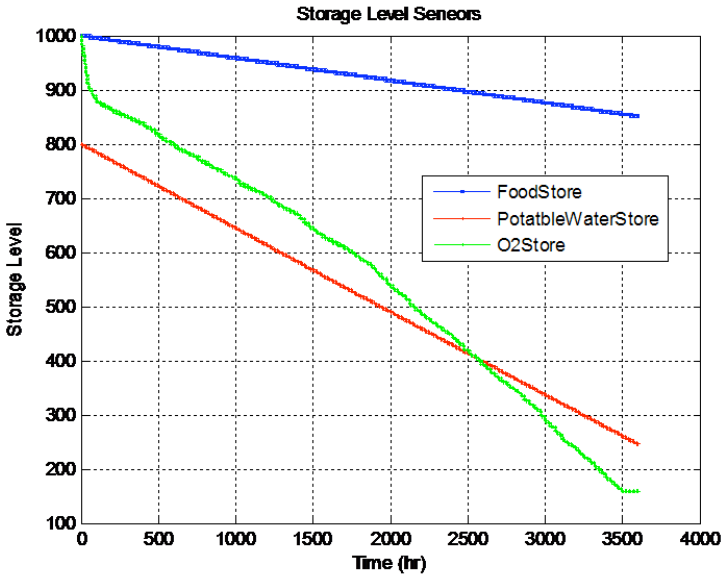



**Figure 17. Store Level Sensors**

# References


[1]Anonymous, "President Bush Announces New Vision for Space Exploration Program," http://www.whitehouse.gov/news/releases/2004/01/20040114-1.html, January 2004.

[2]Perera, J. and Field, S., "Integrated Risk Management Application (IRMA)," 2005.

[3]Anonymous, "Risk Management : Futron Integrated Risk Management Application (FIRMA)," http://www.futron.com/risk*management/tools/futronintegratedriskmanagementapplication.htm*, *Accessed last* : *July* 2008.

[4]Stamatelatos, M., "Probabilistic Risk Assessment: What Is It And Why Is It Worth Performing It?" Tech. rep., NASA Office of Safety and Mission Assurance, 2000.

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

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

[7]Bussolini, J. J., "High Reliability Design Techniques Applied to the Lunar Module," Lecture Series no. 47 on Reliability on Avionics Systems, September 1971.

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

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

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

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

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

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

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

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

[16]Kortenkamp, D. [redacted]ell, S., "BioSim: An Integrated Simulation of an Advanced Life Support System for Intelligent Control Research," 2003.

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

[18]Rodríguez, L. F., Bell, S., and Kortenkamp, D., "Using Dynamic Simulations and Automated Decision Tools to Design Lunar Habitats," 2005.

[19]Rodríguez, L. F., Jiang, H., Bell, S., and Kortenkamp, D., "Testing Heuristic Tools for Life Support System Analysis," July 8 2007.

[20]Jiang, H., Bhalerao, K., Soboyejo, A., Bell, S., Kortenkamp, D., and Rodríguez, L. F., "Modeling Stochastic Performance and Random Failure," July 8 2007.

[21]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.

[22]Hanford, A. J., "Advanced Life Support Baseline Values and Assumtions Document," Tech. rep., 2004.

[23]Anonymous, "http://en.wikipedia.org/wiki/Elektron$(ISS)$,$''$ *Wikipedia*, *Accessed last* : *July* 2008.

[24]Drysdale, A., "Life Support Lessons-Learned from ISS and STS Programs and Foreign Capabilities," Sima teleconference report, Boeing, September, 2006.

[25]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.