Design and Application of the Exploration Maintainability Analysis Tool

Chel Stromgren[1] and Michelle Terry[2]
Binera, Inc., Silver Spring, MD, 20910

William Cirillo[3] and Kandyce Goodliff[4]
NASA Langley Research Center, Hampton, VA, 23681

and

Andrew Maxwell[5]
Georgia Institute of Technology, Hampton, VA, 23666

Conducting human exploration missions beyond Low Earth Orbit (LEO) will present unique challenges in the areas of supportability and maintainability. The durations of proposed missions can be relatively long and re-supply of logistics, including maintenance and repair items, will be limited or non-existent. In addition, mass and volume constraints in the transportation system will limit the total amount of logistics that can be flown along with the crew. These constraints will require that new strategies be developed with regards to how spacecraft systems are designed and maintained.

NASA is currently developing Design Reference Missions (DRMs) as an initial step in defining future human missions. These DRMs establish destinations and concepts of operation for future missions, and begin to define technology and capability requirements. Because of the unique supportability challenges, historical supportability data and models are not directly applicable for establishing requirements for beyond LEO missions. However, supportability requirements could have a major impact on the development of the DRMs. The mass, volume, and crew resources required to support the mission could all be first order drivers in the design of missions, elements, and operations.

Therefore, there is a need for enhanced analysis capabilities to more accurately establish mass, volume, and time requirements for supporting beyond LEO missions. Additionally, as new technologies and operations are proposed to reduce these requirements, it is necessary to have accurate tools to evaluate the efficacy of those approaches. In order to improve the analysis of supportability requirements for beyond LEO missions, the Space Missions Analysis Branch at the NASA Langley Research Center is developing the Exploration Maintainability Analysis Tool (EMAT). This tool is a probabilistic simulator that evaluates the need for repair and maintenance activities during space missions and the logistics and crew requirements to support those activities. Using a Monte Carlo approach, the tool simulates potential failures in defined systems, based on established component reliabilities, and then evaluates the capability of the crew to repair those failures given a defined store of spares and maintenance items. Statistical analysis of Monte Carlo runs provides probabilistic estimates of overall mission safety and reliability.

This paper will describe the operation of the EMAT, including historical data sources used to populate the model, simulation processes, and outputs. Analysis results are provided for a candidate exploration system, including baseline estimates of required sparing mass

[1] Vice President/Chief Scientist, 912 Thayer Avenue Suite 209, AIAA Member.
[2] Junior Analyst, 912 Thayer Avenue Suite 209, non-AIAA Member.
[3] Senior Researcher, Space Missions Analysis Branch, MS 462, non-AIAA Member.
[4] Aerospace Engineer, Space Missions Analysis Branch, MS 462, AIAA Senior Member.
[5] Graduate Research Student, 100 Exploration Way, AIAA Student Member.

and volume. Sensitivity analysis regarding the effectiveness of proposed strategies to reduce mass and volume requirements and improve mission reliability is included in these results.

Nomenclature

CCAA = Common Cabin Air Assemblies
CDRA = Carbon Dioxide Removal Assembly
CO_2 = Carbon Dioxide
CVV = CO_2 Vent Valve
DRM = Design Reference Mission
ECLSS = Environmental Control and Life Support System
EMAT = Exploration Maintainability Analysis Tool
ISS = International Space Station
LEO = Low Earth Orbit
LiOH = Lithium Hydroxide
LMFAQ = Logistics and Maintenance Frequently Asked Questions
MDC = Maintenance Database Collection
MTBF = Mean Time Between Failures
NASA = National Aeronautics and Space Administration
NEA = Near-Earth Asteroid
ORU = Orbital Replacement Unit
PLOC = Probability of Loss of Crew
PLOM = Probability of Loss of Mission
PRA = Probabilistic Risk Assessment

I. Introduction

THE National Aeronautics and Space Administration (NASA) is continuing to develop and analyze design reference missions for human exploration to destinations beyond low Earth orbit (LEO). Missions to these destinations will be challenging from a Supportability perspective due to the mission duration and the difficulty in accommodating required spares inventory. Constraints on mass and volume factor into the Supportability approach for these deep space missions. Traditional Supportability approaches, such as a supply chain from Earth, may or will not be feasible depending on the destination. Alternate Supportability approaches must be analyzed to understand the impact to deep space mission design and formulation.

Supportability refers to the inherent characteristics of design and operations that enable the effective and efficient maintenance and support of the spacecraft throughout the mission. For the purposes of this paper, Supportability includes reliability, reparability, redundancy, and sparing philosophy, with a heavy focus on maintainability. Maintainability is defined as the probability of performing a successful repair action within a given time. In other words, maintainability measures the ease and speed with which a system can be restored to operational status after a failure occurs.

This paper describes general Supportability challenges for beyond low Earth orbit destinations in Section 2. Section 3 provides a description of the model. The data sources for the model are provided in Section 4. The description of the test case and associated results are discussed in Sections 5 and 6, respectively. Section 7 provides the next steps, including expansion of the model to include all the systems, anticipated analysis, and data collection possible improvements.

II. Supportability Challenges

As NASA seeks to explore beyond low Earth orbit (LEO) to such destinations as the Moon, Near-Earth Asteroids (NEAs), and Mars, challenges to Supportability must be better understood, along with approaches to overcoming these challenges. Missions to many beyond LEO destinations will be months to years in duration; thus the traditional supply chain approach, such as has been implemented for the International Space Station (ISS), will not be feasible. In addition, for many destinations, missions will not include an option for quick abort paths back to Earth. This increases the criticality of the spacecraft systems and increases the demands on the overall spacecraft reliability. There is a very high gear ratio associated with these types of destinations, so any increase in logistics mass has very large associated increase in the required propellant and propulsion system mass. In addition, the effect

of the deep space radiation environment may invalidate the established failure rates of systems and components. All of these challenges must be considered when determining a Supportability approach for deep space missions.

When analyzing Supportability approaches, many factors must be considered. Spacecraft must be designed for accessibility to critical systems and components and for volume allocations for spares, consumables, and tools. Time requirements are a major consideration, including repair time to mitigate failures and to perform planned maintenance requirements. A primary focus of Supportability will be on the amount of maintenance and spare items that must be manifested on the mission in order to ensure the safety of the crew and the reliability of the mission. There will be a large number of critical components and systems in the exploration system, with little or no re-supply during these missions. Therefore, the mass and volume of all maintenance and spares items must be accounted for within the design and development to assure a safe and effective mission.

There is a perception that improved reliability alone could solve the Supportability challenges. While improved reliability should directly reduce required crew time for repair and maintenance mass, improved reliability may *not* substantially reduce the required spares mass. Manifesting of spares is intended to protect against possible failures not simply expected failures. There are a large number of elements on a spacecraft whose failure could lead to mission degradation or loss. Most elements have a relatively long mean time between failures (MTBF). With a few exceptions, any given element is not expected to fail but the Supportability approach must allow for protection against a large number of possible failures. Improved reliability may reduce the number of actual expected failures but may not reduce possible failures to a point where specific spares would no longer be manifested.

Reliability is not the only strategy for solving the Supportability challenges for beyond LEO missions. Proposed strategies should focus not only on reducing the number of failures but also on improving maintainability and on reducing the total mass and volume required for spares. These strategies include[i]:

- Lower level of repair - Provide opportunity and capability for the crew to repair failed equipment at lower levels, replacing only the failed element rather than the entire unit
- Commonality - Design systems to utilize similar units or repair items
- Repair during assembly - Provide for a concept of operations that allows all system failures to be repaired and spares stocks replenished immediately prior to departure to the destination
- Redundancy - As an alternative to repair, provide for backup or degradable capabilities
- In-space manufacturing - Provide capabilities to manufacture replacement parts or tools
- Cannibalization and asset reallocation - Scavenge parts from expired modules prior to jettison or discard to build up spares stock

An integrated effort is needed to balance these options into a consolidated approach that provides for a safe and effective mission with acceptable spares mass and volume and crew time requirements.

III. Model Description

In an effort to understand the effects of the various Supportability strategies, Exploration Maintainability Analysis Tool (EMAT) was developed. It performs probabilistic simulation of spacecraft system failures and repair activities. The tool is used to evaluate the reliability and safety of exploration systems by evaluating the impact of system design, reliability of system components, quantity and mix of manifested spares, and reparability of systems.

The operations of spacecraft systems are modeled in EMAT as a set of components linked by logical operational statements. The logic defines how each component contributes to the operation of the system and the impact on the mission and the crew if each component fails. Based on the logic, the tool simulates the operational status of each modeled system in the exploration spacecraft; simulating the occurrence of potential failures and evaluating the capability to repair those failures. Component reliability and spares data is entered into the model and used to evaluate system operations.

EMAT performs stochastic analysis on the modeled systems, modeling potential failures that could occur during a mission, repair activities to respond to those failures, and mission outcome. A Monte Carlo approach is used in EMAT to stochastically evaluate mission reliability and safety. As part of a Monte Carlo analysis, EMAT runs a large number of individual cases, each simulating a potential mission profile with stochastic failures and the related repair activities. The tool then statistically integrates results across the stochastic cases to develop probabilistic estimates for reliability and safety.

The EMAT is structured in several nested layers, each of which executes a different nested level of analysis. Figure 1 illustrates the structure of the model. The model inputs define the system and available spares. System operations are simulated through logical relationships between the components of the system. An entire mission is simulated on a day-by-day basis for a specified mission length. System failures and repair activities are included in this simulation. The Monte Carlo engine executes a large number of mission simulations and the post-processor

summarizes the results. A sensitivity analysis of many Monte Carlo runs with varied input quantifies the impact of the spares mix and system design on mission outcome.

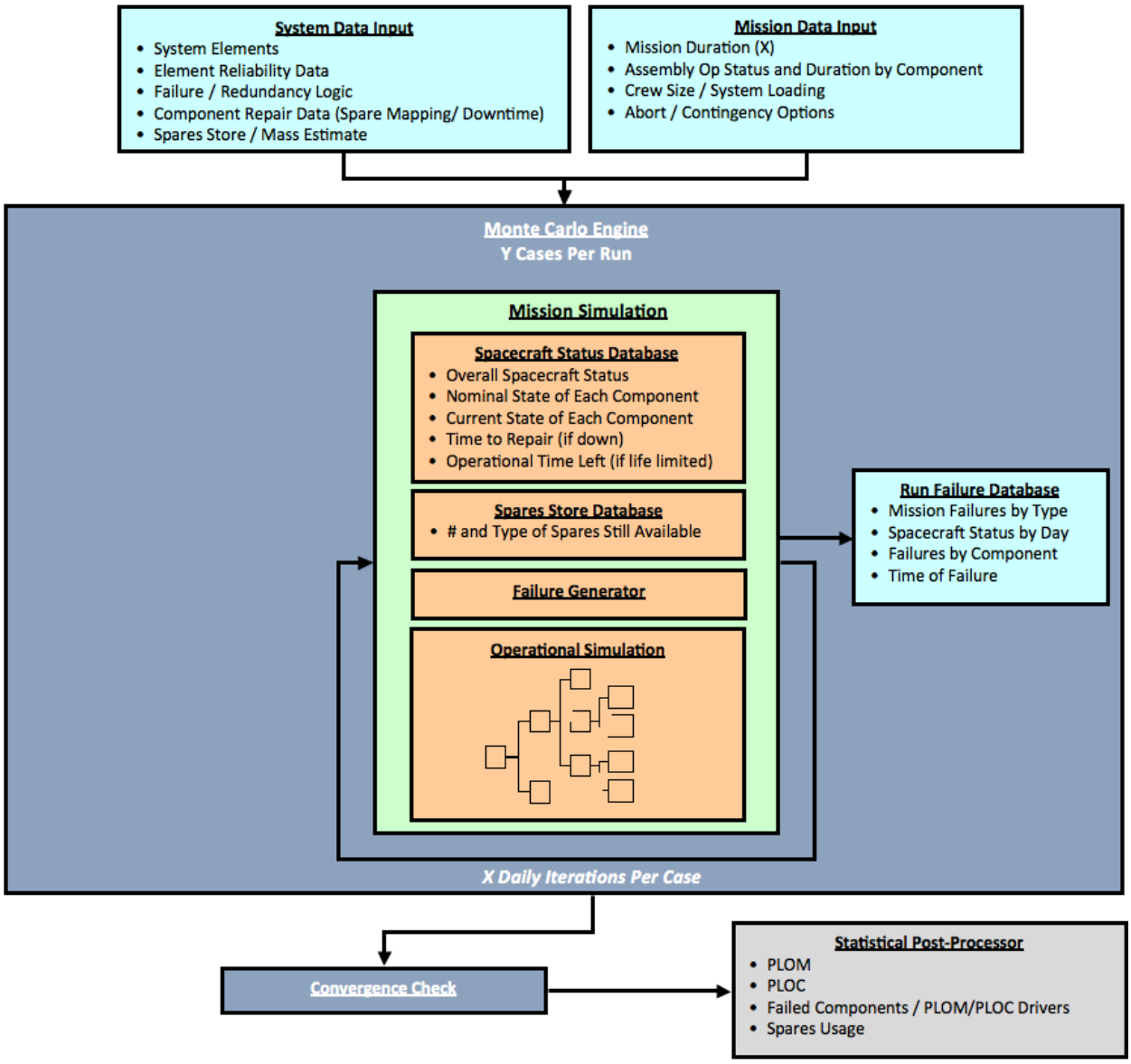

Figure 1. Exploration Maintainability Analysis Tool Structure

A. Inputs

The model requires several types of input: mission duration, abort options, crew size, system description, component reliability data, repair activity data, and spares information. Mission duration and crew size will drive the mass and volume requirements of the limited life consumables.

Spacecraft systems are composed of sub-systems that contribute to the spacecraft's overall function and mission success. At the lowest hierarchical level, systems are composed of base elements. In the EMAT, systems are defined by the logical relationships between base elements and parent elements. Base elements can be individual hardware components or systems, but are treated as the smallest element of a system that can fail and be replaced. For each base element defined in EMAT, corresponding values are entered for reliability, expressed as the element's MTBF, and repair time. Data is entered describing the spare required to replace each element, including the name of the appropriate spare and the mass and volume of that spare. Spares need not be specific to a single element but could be common across multiple elements. Base elements can also be defined as limited-life items, such as systems that

rely on consumables to function. These items do not have MTBFs but are exhausted at the end of their lifetime, which the user must also specify.

The user also defines parent elements, which are systems or functions that are made up of at least two base elements or other parent elements. The user defines the mission state that would result from failure of each parent element. Mission states could include: degraded utilization, degraded crew conditions, loss of mission due to abort, or loss of crew.

The relationships between base elements and parent elements are specified using a standard set of logical statements. The user specifies which base elements and parent elements are related and whether a parent element functions only when all child elements are operating ("AND" relationship), any child elements are operating ("OR" relationship), or whether certain child elements operate only when another child element has failed ("XOR" relationship).

B. Operational Simulation

The most basic level of simulation in EMAT is the Operational Simulation. This level simply determines the response of the system when failures occur. The EMAT simulates the operation of spacecraft systems by integrating all of the elements and their logic relationships into a single system. EMAT evaluates which elements are currently non-operational and uses the logic to determine the status of all other elements and of the overall system. It then evaluates the overall mission state that results from the system failures. As part of the operational simulation, backup elements, which are normally not operating, can be activated if primary elements have failed.

As part of the operational simulation, EMAT also evaluates the activities required to repair a failed element. This includes a check of the defined spares inventory to see if the required spare is available and, if so, an estimate of the required time to repair.

C. Mission Simulation

The next level of simulation in EMAT is the Mission Simulation. This level controls the Operational Simulation in order to simulate an entire mission. The EMAT simulates failures and response to failures on a daily basis over the course of the simulated mission. The one-day period is a balance of accuracy and efficiency. It is difficult to estimate historical element repair times at an accuracy of less than one day. In addition, simulating every hour of a mission lasting several months would also be problematic in terms of processing time. Therefore, a one-day increment presents a good balance of accuracy and efficiency.

On each day of the mission, the EMAT checks the initial system status for that day, carried over from the previous day. It then simulates failures in the system for that day. Based upon the defined reliability data for each element, EMAT simulates random failures in those elements for that day. The model then executes the operational simulation, based on those failures and on failures carried over from previous days. Based on the simulation the model determines overall system status and mission state for that day. If any elements fail, the tool checks if required spares are available and estimates the repair period. If the spare is available then the spare store is decremented and the element is logged as being down for a certain number of days. It is assumed that failed elements are not repaired and reused during the mission. Finally, the model updates repair times for any elements that failed in previous days and are currently being repaired. The mission simulation ends if a failed element with no available spares causes a loss of crew.

D. Monte Carlo Engine

The Monte Carlo Engine is the highest simulation level in EMAT. The Monte Carlo Engine controls the Mission Simulation, executing a series of simulated missions and collecting data on each mission. It records the final mission status, the element that contributed to a mission failure, if applicable, and the spares consumed for each mission. A convergence test is integrated into the Monte Carlo engine to guide the number of mission runs that are executed. The convergence test monitors several key parameters dynamically as the runs are being executed. When the deviation in parameters between runs falls below a pre-defined level of variance, the runs are halted.

E. Post-Processor

The post-processor sits outside of the Monte Carlo engine and performs a statistical analysis across data collected from all of the Monte Carlo simulations. It records the average number of failures, average downtime, and percent of downtime for each base component that is not a limited-lifetime item. For these elements, the post-processor records the average remaining lifetime and average days exhausted. This data can inform spare selection for future runs of the tool. The post-processor also analyzes spare usage to quantify the impact of spare mass on

Probability of Loss of Crew (PLOC). When a sensitivity analysis is performed, this data is used to determine an optimal spares combination where both PLOC and spares mass are within acceptable limits.

IV. Data Sources

Because the design of exploration missions and systems is still in the conceptual stages, it is not yet possible to develop absolute predictions for a mission's reliability and safety. Rather, the intended purpose of EMAT is to evaluate the sensitivity of exploration system Supportability to a variety of design factors. However, the efficacy of the tool is still heavily dependent on the availability and quality of the data used in the analysis. Data used to populate EMAT is taken primarily from ISS design and operational experience. The ISS provides a source of risk information regarding long-duration spacecraft systems. Although the ISS is larger and more complex than anticipated exploration systems, many of the systems will be similar in design. Data at the component level, including reliability data, repair data, and spares data will be applicable to exploration systems. ISS-based data are used to derive each of the primary inputs to EMAT.

Logical System Descriptions **-** The most basic set of data used to model exploration systems in EMAT are the logical operational descriptions of the spacecraft systems. For most systems, the descriptions are initially derived from the logical descriptions contained in the ISS Probabilistic Risk Assessment (PRA). The PRA for ISS Stage 7A configuration was used as the basis for modeling[ii]. This configuration, which represents the configuration of the ISS during construction, after assembly flight 18 (December 7, 2001), was selected because it more closely represents anticipated exploration systems than the Assembly Complete ISS.

The PRA model details how failures at the component level can propagate through the system as a whole and result in an undesirable end state, such as loss of system or loss of crew. System fault trees are linked to repair attempts as part of the event sequence diagrams, which represent the highest level of configuration information for the PRA. These diagrams take into account functionally redundant systems, which support critical ISS functions and must all fail for a negative end state to be reached.

The logical descriptions in the PRA were used as the starting point for developing the Logical System Descriptions for EMAT. System descriptions were modified as appropriate to match the currently anticipated system design for the exploration spacecraft. In many cases, anticipated exploration systems will be simpler than the equivalent systems on ISS. In addition, it is anticipated that new technologies will be incorporated into exploration systems. In this case, the logical descriptions were modified to align with these changes.

Certain exploration systems, particularly propulsion systems, are not present on the ISS and therefore are not represented in the PRA. In these cases, logical system descriptions were developed based on the best current description of those systems. In most cases, these descriptions are not defined to as fine a level of specificity as those derived from ISS.

Component Reliability **–** Reliability estimates for each modeled component are a primary input to EMAT. There are two primary sources for component reliability data. The first is the ISS PRA, which contains an estimate of individual component failure likelihood and its associated uncertainty for all components. For some components the reliability estimates in the PRA, which were developed prior to ISS construction, have been updated based upon the decade plus of real-world flight experience of ISS. These updates, developed using Bayesian analysis, are captured in the NASA ISS Program Office's Orbital Replacement Unit (ORU) Logistics and Maintenance Frequently Asked Questions (FAQ) database (LMFAQ) catalog. Where available, these updated estimates were used in EMAT.

Spares Mass and Volume **-** Information regarding system spares is necessary for the tool to be able to evaluate the spares inventory. The LMFAQ database was used to identify spares for modeled components and to compile the mass and volume estimates for each spare. This database catalogs all of the current spares for the ISS, both on the ground and on board. It contains mass, volume, and inventories for most of the components considered in the PRA.

Repair Time **-** The NASA ISS Program Office's Maintenance Database Collection (MDC) was used to derive repair time estimates for all modeled components. The MDC catalogs every maintenance and repair activity that has occurred on ISS and captures the time required for these activities, both in terms of astronaut hours expended on the task and total time required to restore a component to operation. While this is very useful information, it lacks contextual information such as other crewmember responsibilities, other maintenance demands, and repair priority of the actions recorded. As a result, it is difficult to gage how long the physical act of repairing and replacing the item takes independent of all the other demands on the crew. Best engineering judgment was applied to the estimates

derived from the MDC and the precision of the estimates was limited to one day. In cases where specific components have not been repaired on ISS, data for analogous components was used to derive estimates.

V. Test Case

In order to evaluate and demonstrate the functionality and utility of the EMAT, a single spacecraft subsystem was selected for initial testing. Building and evaluating a test model with a tractable scope allowed for demonstration of the capabilities of the tool, testing and refinement of the tool's functionality, and validation of the results without being overburdened with modeling a complex system.

For this study, a carbon dioxide (CO_2) removal system for the exploration habitat was modeled. This system is life critical to the crew and is relatively self-contained. In addition, the characteristics of the CO_2 removal system allow for full testing of the functionality of EMAT. The CO_2 removal system is highly critical, it is likely to incorporate some level of build-in redundancy, relies on consumables for contingency operations, and historically it has been subject to failures. Finally, CO_2 removal is a fairly mature technology. While there may be some improvements in materials and/or reliability for future exploration, it is not anticipated that there would be a fundamental change in the operations of the system. This allows modeling of the system to be based on historical operational and system data.

The logical model of the CO_2 removal system for the exploration vehicle was initially based upon the design of the ISS CO_2 removal system. Although the anticipated system for the exploration vehicle would not be an exact copy of the ISS system, it is possible to derive a model of the exploration system starting from the ISS design.

On ISS CO_2 removal is accomplished by two redundant primary systems: the Vozdukh on the Russian Segment and the Carbon Dioxide Removal Assembly (CDRA) on the U.S. segment. Lithium Hydroxide (LiOH) canisters are used as a contingency backup if both of these systems fail. The Vozdukh and CDRA both use a dual swing bed system to remove CO_2.

The ISS CO_2 removal system model was modified in several areas in order to align more closely with the anticipated design of a long-term mission. The main deviation from the ISS design was that the redundant Vodukh was removed from the system. While fully redundant systems could be used in an exploration spacecraft, this would result in a high mass. Therefore, the EMAT model includes only a CDRA and a backup LiOH system. It is anticipated that redundancy at the element level might be used and this option was evaluated as part of this effort.

The modeling of the system in EMAT was also simplified in a few other areas. The scope of the model was limited to elements that were integral to the CO_2 removal system itself. Therefore, failures that could impact the operation of the CO_2 removal system, but occur in other systems, were not modeled. For the CO_2 system, these external failures include power failures, thermal system failures, and computer system failures. In addition, software failures were not modeled as they are outside of the scope of the model. The linkages between systems are important to overall reliability and safety and will be captured in future implementations of the model as other systems are included.

The CDRA's main components are a set of two desiccant/sorbent beds for adsorption and desorption of water and CO_2. The two Common Cabin Air Assemblies (CCAAs) provide air to the CDRA. Inlet air first passes over a desiccant bed that adsorbs water and then is pumped over a sorbent bed that adsorbs CO_2. Simultaneously, the second sorbent bed is heated and CO_2 that has been adsorbed in the previous cycle is vented overboard through the CO_2 Vent Valve (CVV). Once all water and CO_2 has been adsorbed from the inlet air, the air passes over the saturated desiccant bed. The water is desorbed and the air is re-humidified for return to the cabin to conserve water. Extra air is also pumped from the desorbing CO_2 sorbent bed back into the cabin to conserve oxygen. The desiccant/sorbent beds cycle from adsorption to desorption every 144 minutes[iii]. Figure 2 shows a schematic of the CO_2 removal system used in this pilot study.

One additional change to the CDRA was modeled as an option for this analysis. This option involved the addition of a third redundant desiccant/sorbent bed to the CDRA model. Two desiccant/sorbent beds must be operating in order for the CDRA to function. However, these beds have experienced a high degree of failure. It might therefore be desirable to have an internal spare that can be quickly activated rather than having to shut down the system to replace the failed bed.

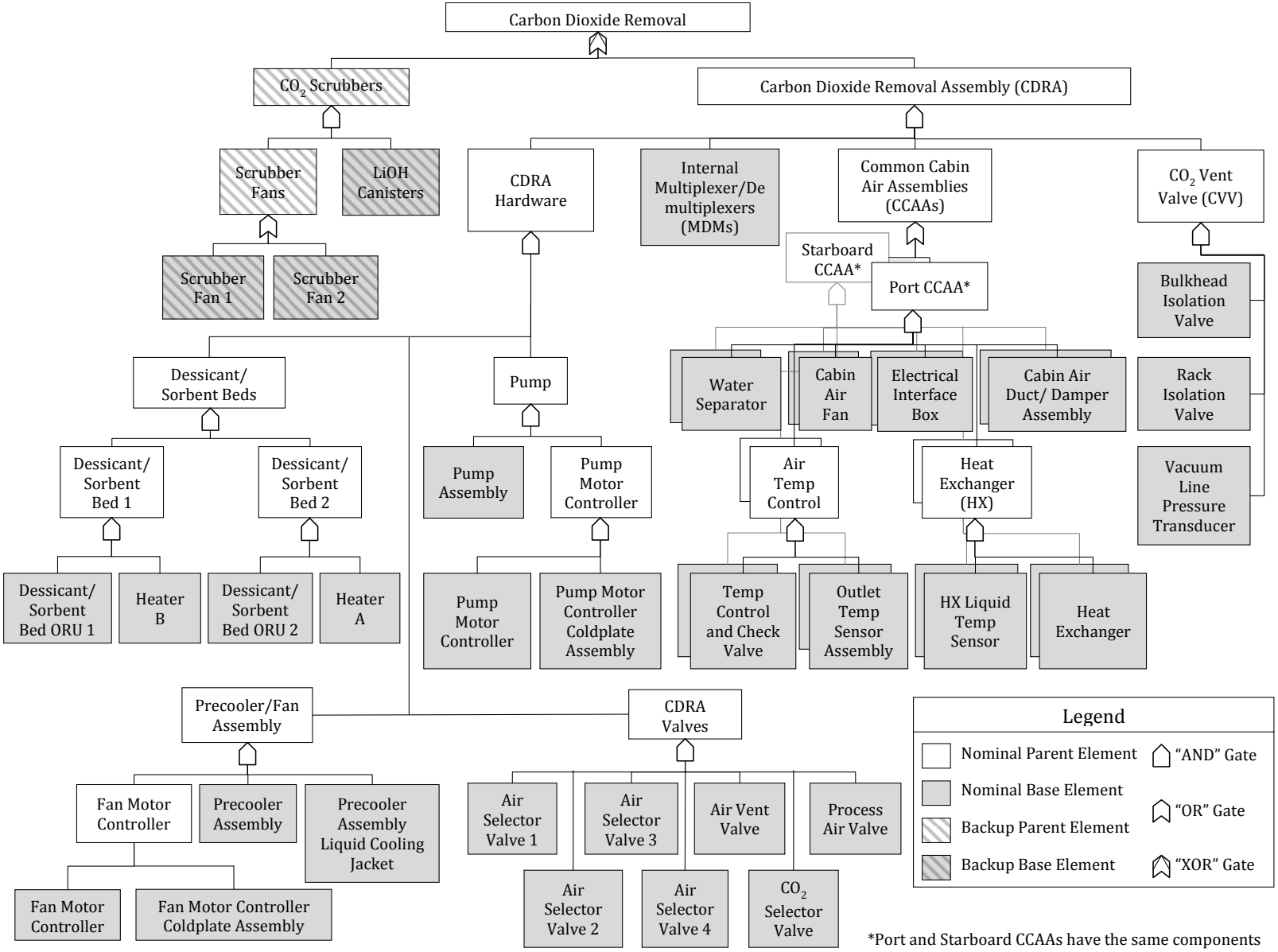

Figure 2. Schematic of Carbon Dioxide Removal System tested in the EMAT

VI. Test Case Results

The results of the EMAT analysis for the carbon dioxide removal system illustrate the functionality and utility of the tool. The EMAT was used to evaluate the impacts of reliability and reparability of the carbon dioxide removal system on overall mission reliability and safety. In addition, the tool was used test the effect of factors such as individual component reliability, spares inventory, and system redundancy on the mission.

For the test analysis a representative mission with duration of 365 days was evaluated. This duration represents the length of a challenging mission to a NEA but could also represent other classes of exploration missions. The duration can easily be altered in EMAT to evaluate other mission types.

For the purposes of this analysis, it is assumed that evaluated systems are all fully functional and the spares inventory is fully stocked at the beginning of the simulated duration. This means that any failures that occur during the launch and assembly period are corrected prior to departure. This assumption could be traded in the future as part of optimizing the mission. In addition, it was assumed that this mission had no abort options, so no accelerated return to Earth was considered.

Because the actual CO_2 removal system for an exploration vehicle has not yet been designed, it is not possible to predict achieved specific levels of mission reliability and safety. Rather, the potential impacts of various design and operational decisions on the reliability and safety are evaluated through sensitivity analyses. These analyses allow designers to understand the impacts of different configurations and options on the mission.

Four types of sensitivity analysis were conducted on carbon dioxide system reliability and safety:

1. Spares inventory on the spacecraft
2. Contingency consumables inventory
3. Integration of redundant components in the system
4. Component reliability

A. Spares Inventory on the Spacecraft

An evaluation of the types of spares manifested on the mission and the total mass of spares dedicated to the CO_2 system was the primary analysis completed as part of this effort. Spares mass is a critical factor in mission design and the inventoried spares will have a major impact on mission safety.

An iterative approach was used to evaluate the relationship between spares inventory and overall mission safety. An initial stochastic run was completed with no spares inventoried on the spacecraft. This run, predictably, resulted in a very high predicted PLOC during the mission. The results of the cases were then statistically evaluated to determine how different component failures contributed to the overall probability of system failure. The contribution of each element was then compared to the mass of the spare required to repair that failure. The spare that had the greatest potential contribution to reduced PLOC per kg of mass was identified. That spare was then added to the spare inventory that was input into the model and the stochastic analysis was re-run. This process was repeated until improvements in PLOC were no longer statistically significant. The result was a series of potential cases, each involving a different mix of spares, and with increasing level of safety and mass.

Because the operational relationships in the CO_2 removal system are quite complex, the method used to increment the spares might not necessarily yield the optimal combination of spares for any given mass. For this reason, alternate combinations of spares were run at each point, changing the mix slightly. The results for all evaluated spares inventories were then plotted on a scatter diagram. The mission PLOC was plotted against the total inventories spares mass for that system, including contingency LiOH canisters. An efficient frontier, representing the cases that produced the lowest PLOC for any given spares mass, was found in the data and only those points on the efficient frontier are plotted in this paper.

For this analysis, 15 days of contingency LiOH canisters were included in the initial inventory and no redundant components were added to the system. Reliability values for all components were set to the baseline ISS historical values. The results for this run are shown in Figure 3.

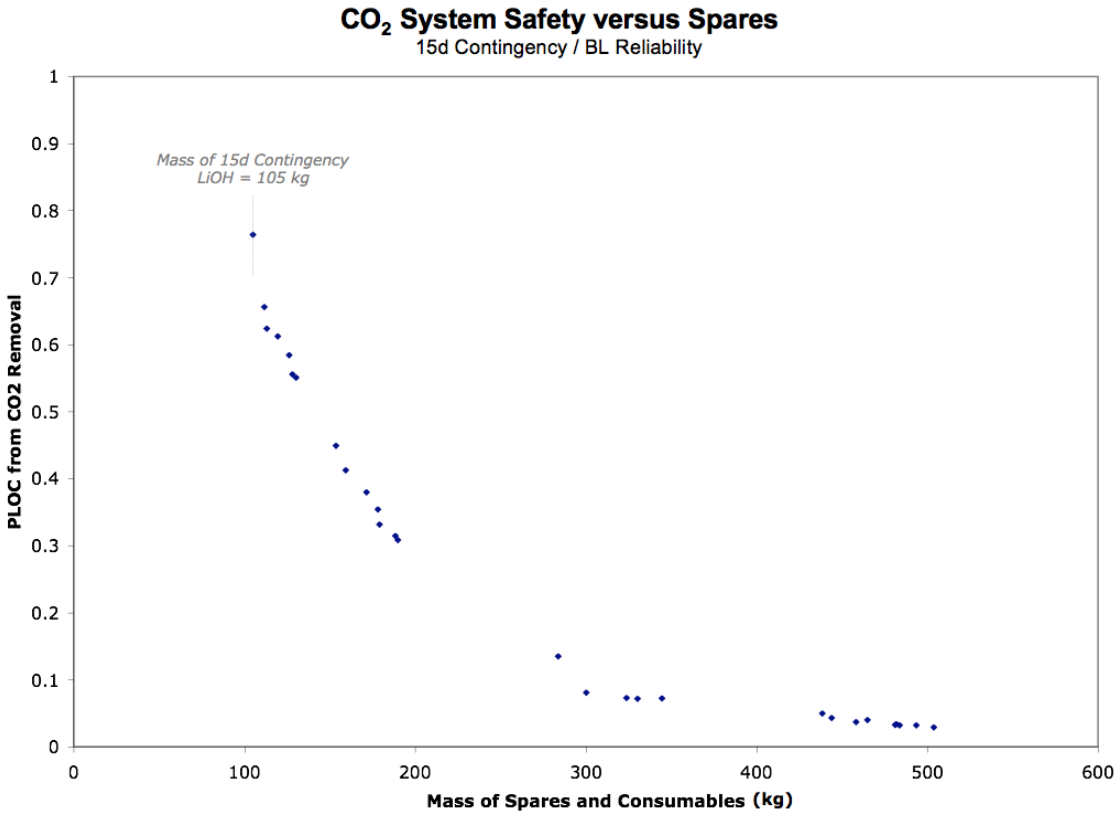

Figure 3. Spares Inventory on the Spacecraft Analysis Results – Baseline (BL) Reliability

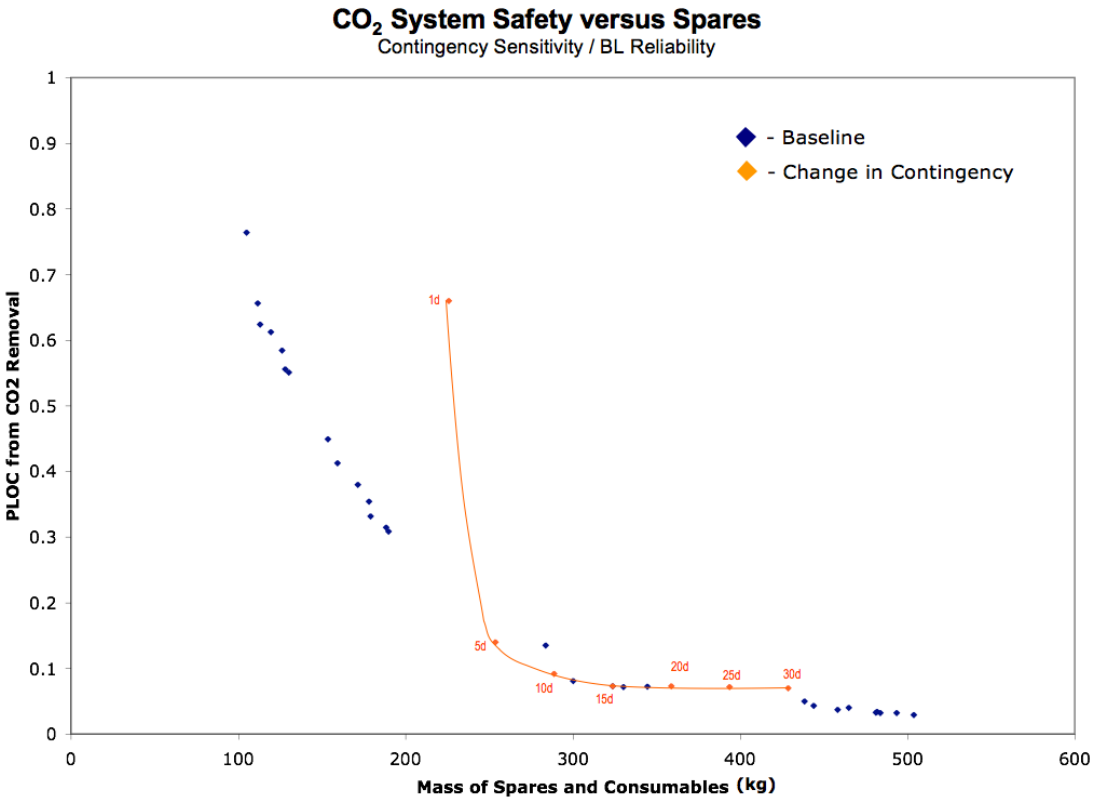

Figure 4. Contingency Consumables Analysis Results – Baseline (BL) Reliability

In Figure 3, it can be observed that the predicted PLOC for the mission, attributed solely to failure of the CO_2 removal system, is 0.76. This means that, with no spares beyond the LiOH canisters, that there is a 76% probability that the mission would end in loss of the crew due to failure in the CO_2 removal system. As spares mass is added, the predicted PLOC drops rapidly, as the highest frequency failures become repairable. Then, as the frequency of the component failures that are being covered drops, the rate of improvement in PLOC drops.

At a total spares mass of 480kg for this system, the PLOC contribution is 0.03. Only very small improvements in PLOC are achievable by increasing spares beyond this point. At some point, manifesting additional spares will become less efficient than simply adding more contingency LiOH canisters.

B. Contingency Consumables

The EMAT was used to evaluate the impact on safety of the amount of LiOH canisters that are manifested on the mission. The LiOH system is an emergency backup to the CDRA and uses consumable canisters to remove CO_2 from the atmosphere. The canisters modeled in the system are the same as those used on the ISS and, when in use for contingency operations, are consumed at a rate of 1.75 kg per crewmember per day.

The impact of manifesting additional LiOH canisters on a mission is different from adding component spares. LiOH canisters protect against periods where the CDRA system is down for repair but will not protect the crew from non-reparable component failure in the CDRA (unless the quantity of canisters is sufficient to last all the way back to Earth). However, a certain amount of LiOH is required to allow time for repairs to the primary system.

A spares mix was selected from the baseline assessment that represented a balance of PLOC and spares mass. This mix achieved a PLOC of 0.08 at 300 kg of spares mass. In the baseline case 15 days of LiOH canisters was manifested. For this sensitivity analysis, the inventory of LiOH canisters was varied from 5 days to 30 days in 5 day increments.

Figure 4 shows the results for the LiOH sensitivity analysis at the selected point. These results demonstrate that there will be an optimal inventory of contingency consumables for any given spares mix. That amount must cover the period required to conduct the expected repair activities. For this case, it can be seen that with contingency periods of less than 20 days, there is a rising increase in PLOC. This is because there is a high probability that the available consumables will be exhausted before the end of the mission, therefore the effectiveness of adding spares is reduced. With contingency of 20 days or greater, additional decreases in PLOC are small. The amount of consumables covers most repair activities and added consumables only offer increased protection against failures towards the end of the mission. Theoretically with an inventory of 365 days of LiOH, at a mass of 2,555kg, no CRDA would be necessary and the PLOC would be very small.

It should be noted that the amount of LiOH canisters manifested on this mission is only the amount needed for repair and replace activities. It is possible that other repairs to the CDRA system might take place that do not require replacing a failed element with a spare, but will require shutting down the system and consuming LiOH canisters. These types of repair activities are not considered in this model. Manifesting additional LiOH canisters may be required on missions to provide CO_2 removal during minor repairs.

C. Redundant Components

Designing redundancy into a system is an alternative approach to improving reliability of spacecraft systems. For this analysis, redundancy was considered at the component level, where a spare component is permanently integrated into the system and can be activated in the event of failure of a primary component with a minimum of effort and without having to remove the failed component. The redundant component is not normally operating but can be activated when necessary. Although redundant components tend to add additional mass to the system, beyond what would be required for a cold spare, they can significantly reduce the downtime required for repair. In addition, redundancy reduces the risks involved with repair activities.

On ISS there are two fully redundant CO_2 removal systems, the CDRA in the U.S. segment and the Vozdukh in the Russian segment. This provides a very high level of reliability and safety. For this analysis, redundancy was analyzed at the component level. Although it is possible that there could be fully redundant systems, the resultant system mass would be very high. Therefore it was assumed the redundancy would occur at a lower level.

To demonstrate the impact of redundant components on mission safety, a redundant desiccant/sorbent bed was added to the CDRA. The CDRA normally has two beds, both of which must be working in order for the system to function. These beds have experienced a number of failures on ISS and are critical to system operation.

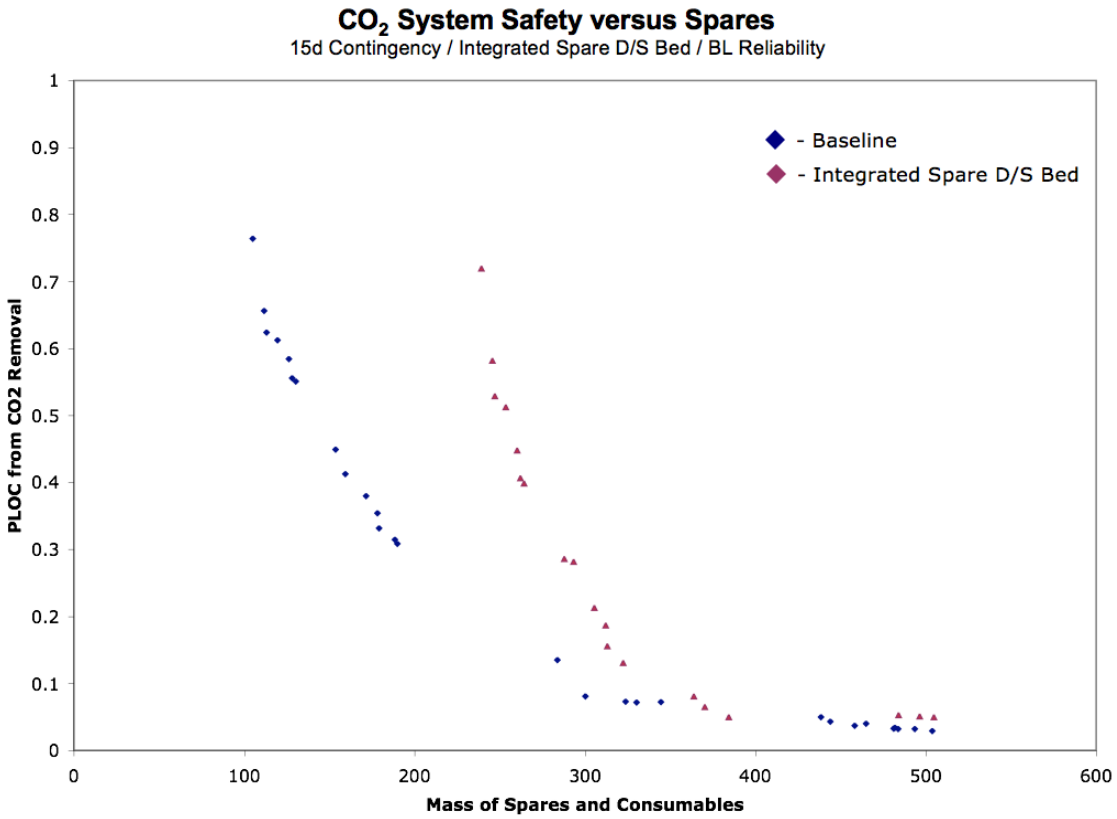

Figure 5. Redundant Components Analysis Results – Baseline (BL) Reliability

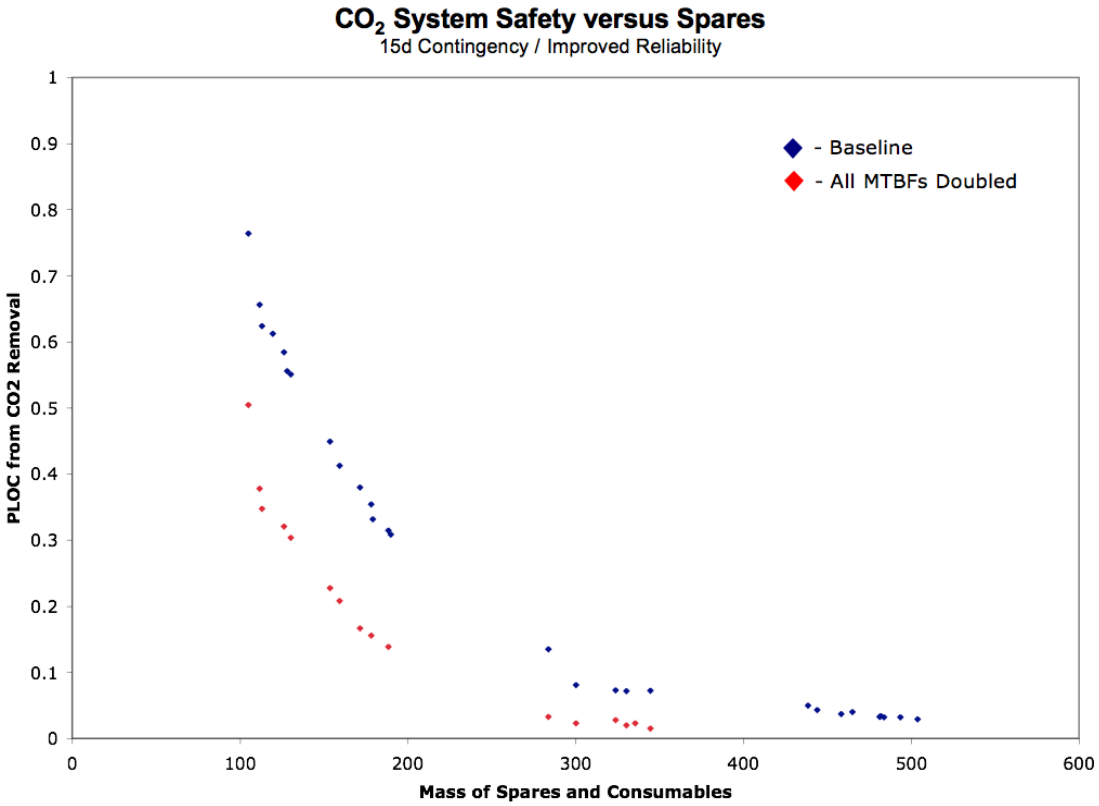

Figure 6. Component Reliability Analysis Results – Improved Reliability

A redundant component would involve a third bed, directly plumbed into the CDRA system. If one of the two primary beds failed, the third bed could be activated and switched into operation. If the failed primary bed could be repaired, it could then be returned to operation and the redundant bed switched off, or the primary could become the new redundant bed.

The spares allocation process, described above, that was used to evaluate the trade-off between spares and PLOC was repeated with the redundant component in the system. The efficient frontiers for the cases with and without the redundant bed were then compared. For these runs, it was assumed that adding the redundant bed would result in a mass increase to the CDRA system of 94 kg for the spare desiccant/sorbent (D/S) bed and 40 kg for associated integration hardware. Figure 5 shows the results of this analysis. In this figure the additional mass of the D/S bed and associated hardware is included in the total spares mass. From Figure 5, it can be observed that the addition of a redundant spare is inefficient at low spares mass allocation. In that range, the increase in PLOC due to the redundant spare is more than offset by the additional required mass. It would be more efficient to use that mass to manifest other critical spares. With larger spares mass allocation, the redundant component improves overall efficiency by reducing the amount of repair time required, thus reducing the probability that contingency consumables are exhausted.

D. Component Reliability

The final sensitivity analysis that was completed evaluated the impact of component reliability on overall mission safety and reliability. It is anticipated that systems incorporated into future exploration spacecraft will have improved levels of reliability, as compared to the current state of the art. Improved reliability will be key to reducing required spares and to limiting the amount of time the crew must spend repairing failures.

However, as discussed earlier, it is anticipated that the reduction in required spares may not be proportional to improvements in reliability. The number of required spares is not directly driven by the failure rate. Spares are not manifested because a component is expected to fail – in fact, given the reliability of components it is unlikely that any given component will fail. Rather, spares are manifested to protect against possible critical failures.

For this sensitivity analysis, the failure rate of all CDRA components was reduced by 50% (MTBF values were doubled). The spares allocation process, described above, that was used to evaluate the trade-off between spares and PLOC was repeated with modified reliabilities. The efficiency frontiers for the cases with ISS reliabilities and improved reliabilities were compared. The results of this analysis are shown in Figure 6.

From Figure 6 it can be observed that a large increase in the reliability of all components would have a major impact on improving overall mission safety. With no spares and 15 days of contingency the PLOC from the CO_2 system was reduced from 0.76 in the baseline run to 0.51. To achieve equivalent levels of risk reduction, the required spares mass was reduced by 25-30%. However, this demonstrates that achieved reduction in mission safety will not be directly proportional to increased reliability.

E. Summary of Test Results

The results of the EMAT analysis demonstrate that maintainability will be a major issue in achieving an acceptable level of reliability and safety for long-duration exploration missions. The complexity and large number of components on a deep space vehicle present many opportunities for failure.

The results of this analysis show that, using ISS heritage hardware, the CDRA system would contribute approximately 2% to PLOC for a one-year mission, with 500 kg of spares dedicated to this system. The CO_2 removal system is just one small part of the overall deep space vehicle. On ISS, failure of the CO_2 removal system constitutes a very small fraction of the total PLOC (primarily because of the redundant nature of the system). Although it is difficult to compare ISS results to predictions for deep-space missions, because of the opportunities for crew abort, these results show that failure of the CO_2 system will represent just a small fraction of the overall PLOC. Similarly, on ISS, spares for the CO_2 system represent less than 1% of total spares manifested on-board the station.

While the use of redundant components, contingency consumables, and improved reliability will reduce the required spares mass, it is anticipated that a significant amount of spares will still be required to achieve an acceptable level of safety. The mass and volume of these spares could be a major design driver for the transportation system.

VII. Extensibility

The EMAT is intended to support mission and element design, starting in the conceptual phase, for future exploration missions by providing analysis of mission safety and reliability, as well as estimates for spares mass and

volume requirements. The tool will support analysis of alternative approaches for improving maintainability and supportability.

The next step in the development of EMAT will be to expand the scope of the modeling effort to incorporate additional systems required for a deep space vehicle, including the Environmental Control and Life Support System (ECLSS), power system, thermal system, command and data handling, etc. The model should ultimately include all systems that could contribute to degraded mission state, loss of mission, or loss of crew.

Once all the applicable systems are modeled within EMAT, the model can be used to estimate the total maintenance and repair mass required to achieve different levels of overall mission reliability for proposed exploration missions concepts and types. Human exploration DRMs can be evaluated with different maintenance and sparing strategies, including level of repair, repair item inventory, and level of redundancy. This will help inform the mass and volume requirements needed for spares.

An important aspect of maintainability will focus on the benefits of moving towards lower level repair of spacecraft systems. Conceptually, the mass of required spares can be substantially reduced by repairing failed components rather than replacing them. This would involve diagnosing failures within a component and then replacing only the specific sub-element(s) that have failed. Because only certain parts of each component are subject to failure, the total required mass of the spares could be reduced by pursuing this approach. It will be important to extend EMAT to enable evaluation of the impact of moving to lower level repair. Modeling this approach would require an increased level of definition of the logical models in the tool. Rather than evaluating failures at the component level, the tool would have to simulate failures at the sub-element level. This would require modeling of the logical operations within each component.

The model will also be extended to include analysis of crew time requirements for maintenance and repairs. Limitation on crew time available for repairs could also be a driving factor in Supportability. While total repair duration is currently captured in the model, the amount of total crew hours dedicated to maintenance and repair activities is not. Capturing crew time impacts will be particularly important when evaluating lower-level repair, where crew time demands will be more intensive.

An additional area of focus will be on evaluating the impacts on commonality on spares mass and volume. Commonality potentially reduces the number of required spares, since common spares can be used to cover a number of potential failures, rather than manifesting specific spares for each component. In order to evaluate the impacts of commonality, it will be necessary to identify commonality opportunities across all spacecraft sub-systems. These opportunities can then be captured and analyzed in EMAT. However, in order to accurately assess the net impacts, it will be necessary to capture the added system mass required to facilitate the use of common components. A related issue that needs to be integrated into the EMAT analysis is an assessment of potential impacts from common-cause failures on overall system reliability and safety. Currently, all failures are treated as being independent within EMAT. In actual operations, there are often linkages between failures, resulting from common root causes. Additional logic will be incorporated within EMAT to modify the reliability of components based on previous failures.

In addition to model development, there will be an effort to improve the accuracy of the data. This will be achieved by continuing to capture ISS operational experience and accessing other analog data sources.

Acknowledgments

The authors would like to acknowledge the ISS Logistics & Maintenance Office at Johnson Space Center for providing ISS data and sharing their acquired knowledge.

References

[i] Cirillo, W., Goodliff, K., Aaseng, G., Stromgren, C., and Maxwell, A., "Supportability for Beyond Low Earth Orbit Missions," AIAA Space 2011 Conference and Exposition, AIAA-2011-7231, Long Beach, CA, September 2011.

[ii] Futron Corporation "Probabilistic Risk Assessment of the International Space Station: Phase II- Stage 7A Configuration," ISS PRA Phase II Report, Dec 2000

[iii] Murdock, K., "Integrated Evaluation of Closed Loop Air Revitalization Systems," Marshall Space Flight Center, NASA/CR-2010-216451, November 2010, pp. 6-7.