The Threat of Uncertainty – Why Using Traditional Approaches for Evaluating Spacecraft Reliability Are Insufficient for Future Human Mars Missions

Chel Stromgren[1]
Binera, Inc., Silver Spring, MD, 20910

Kandyce Goodliff[2] and William Cirillo[3]
NASA Langley Research Center, Hampton, VA, 23681

and

Andrew Owens[4]
Massachusetts Institute of Technology, Cambridge, MA, 02139

Through the Evolvable Mars Campaign (EMC) study, the National Aeronautics and Space Administration (NASA) continues to evaluate potential approaches for sending humans beyond low Earth orbit (LEO). A key aspect of these missions is the strategy that is employed to maintain and repair the spacecraft systems, ensuring that they continue to function and support the crew. Long duration missions beyond LEO present unique and severe maintainability challenges due to a variety of factors, including: limited to no opportunities for resupply, the distance from Earth, mass and volume constraints of spacecraft, high sensitivity of transportation element designs to variation in mass, the lack of abort opportunities to Earth, limited hardware heritage information, and the operation of human-rated systems in a radiation environment with little to no experience. The current approach to maintainability, as implemented on ISS, which includes a large number of spares pre-positioned on ISS, a larger supply sitting on Earth waiting to be flown to ISS, and an on demand delivery of logistics from Earth, is not feasible for future deep space human missions. For missions beyond LEO, significant modifications to the maintainability approach will be required.

Through the EMC evaluations, several key findings related to the reliability and safety of the Mars spacecraft have been made. The nature of random and induced failures presents significant issues for deep space missions. Because spare parts cannot be flown as needed for Mars missions, all required spares must be flown with the mission or pre-positioned. These spares must cover all anticipated failure modes and provide a level of overall reliability and safety that is satisfactory for human missions. This will require a large amount of mass and volume be dedicated to storage and transport of spares for the mission. Further, there is, and will continue to be, a significant amount of uncertainty regarding failure rates for spacecraft components. This uncertainty makes it much more difficult to anticipate failures and will potentially require an even larger amount of spares to provide an acceptable level of safety. Ultimately, the approach to maintenance and repair applied to ISS, focusing on the supply of spare parts, may not be tenable for deep space missions. Other approaches, such as commonality of components, simplification of systems, and in-situ manufacturing will be required.

[1] Vice President/Chief Scientist, 8455 Colesville Road Suite 1075, AIAA Member.
[2] Aerospace Engineer, Space Missions Analysis Branch, MS 462, AIAA Senior Member.
[3] Senior Researcher, Space Missions Analysis Branch, MS 462, non-AIAA Member.
[4] Graduate Research Fellow, Department of Aeronautics and Astronautics, Building 33-409, 77 Massachusetts Ave., AIAA Student Member.

Nomenclature

DSH	=	Deep Space Habitat
DSV	=	Deep Space Vehicle
EMAT	=	Exploration Maintainability Analysis Tool
EMC	=	Evolvable Mars Campaign
ISM	=	In-Space Manufacturing
ISS	=	International Space Station
LEO	=	Low Earth Orbit
MTBF	=	Mean Time Between Failure
NASA	=	National Aeronautics and Space Administration
PLOC	=	Probability of Loss of Crew

I. Introduction

THROUGH an investment in the Evolvable Mars Campaign (EMC)[i], NASA continues to study human missions beyond low Earth orbit (LEO) and on to Mars in the 2030s. One of the major challenges with missions to Mars will be keeping the spacecraft operational for long durations away from Earth to the degree necessary to meet Agency safety expectations. How the spacecraft is maintained and repaired in transit and at the destination will have a major impact on safety and reliability. Current approaches to maintenance and repair, implemented for the International Space Station (ISS), will not suffice. ISS has the benefit of being in LEO, thus allowing for ease of access. In addition, ISS has a large number of spare components on board and a larger supply waiting on Earth to be launched on-demand, greatly reducing the risk of a non-repairable failure. For missions to Mars, the distance from Earth and duration of the mission will necessitate the need for a different maintenance strategy.

Once the crew departs from Earth's sphere of influence, there will be no opportunity to resupply the deep space vehicle (DSV). Therefore, all the spare components required to maintain a high probability of crew safety and mission success will have to be included with the DSV or pre-positioned. Conjunction class Mars missions (as envisioned in EMC) range in length from 1,000 to 1,200 days, with no quick abort path back to Earth. The duration drives the amount of spares required to protect against probabilistic failures over the mission. The lack of any quick abort paths back to Earth also dictates the need to send all critical spares along with the crew. These missions will have stringent mass and volume constraints due to the energy required to propel the Deep Space Vehicle (DSV) to Mars and back to Earth. Adding mass and volume of the spare components must be balanced with the propellant requirements to transit the DSV to the destination and return them to Earth.

Given that NASA's experience with long-duration crew spacecraft operations is limited to ISS and LEO, several sources of uncertainty exist in the ability to relate ISS reliability heritage information to the design and selection of components to be included in any potential future DSV. These uncertainties are likely to stem from a variety of sources including the potential use of non-ISS heritage systems or the use of ISS heritage systems that haven't operated for a sufficiently long enough period of time to ascertain a statistically valid understanding of their expected lifetimes. This limited operational experience will have a negative effect on NASA's understanding of system reliability in a number of areas including random failures, induced failures, wear out, and potential design and manufacturing errors. Lack of system reliability characterization is further likely to be exasperated given uncertainties in the deep space environment, unknown radiation effects, and the complexity of the system envisioned to support crew on their journey to Mars and back.

II. Uncertainty in Random Failures

Anyone who has ever purchased a new car has likely heard the advice to never buy a model in its first year of production. In fact, statistics generally show that this advice is sound[ii]. The first model year of most vehicles have traditionally experienced higher rates of failure and more recall notices than do later model years. This is true despite the fact that the automobile companies spend large sums of time and money dedicated to testing and improving these vehicles in a relevant environment before they are put into production; i.e., accumulating a large number of test miles before they actually hit the showroom floor.

So, why does this happen? Well, it often comes down to a critical factor called "MTBF, or "Mean Time Between Failures". This parameter predicts the average time between random failures for each component in the car (or any other system). It is NOT a measure of lifetime of the component. If this were true, failures would be easy to address. Through proper testing, the time at which a component will wear out could be predicted and improvements to problematic parts could be made. But, the types of random failures defined by MTBF have nothing to do with accumulated lifetime; rather they are failures that can occur randomly at any time. However, by knowing the MTBF, one should still be able to predict the frequency of failures and would be able to engineer a car that is more reliable from the start.

The potential issue, however, is uncertainty in establishing a statistically valid MTBF. When new products are first developed, one can only make estimates for MTBF. This is done based on a number of inputs including component testing in a relative environment, and on how previously existing similar components (motors, valves, fans, etc.) have performed in similar applications. But, each new component design contributes new uncertainties and each new application introduces a new environment and therefore additional new uncertainties. Because predicted MTBFs are generally very long, the only way to reduce the uncertainty in the estimates is to run a large number of components for very long periods of time. That is why reliability often suffers in the first model year; until thousands of cars have accumulated a large number of miles, there is not enough information available to refine the MTBF estimates and to identify and rectify problem components.

So, how does this impact human travel to Mars?

The Deep Space Habitat (DSH), which is the portion of the DSV designed to house and keep the crew alive for the trip to and from Mars, will be one of the most complex machines ever designed. As currently envisioned, the habitat will close the environmental loop, recycling air and water. It will regulate the temperature of the spacecraft. It will provide power for all necessary functions. It will provide navigation, control, and communications. And, it will provide all of the other functions required to keep a crew healthy and productive for up to three years. The systems of the habitat will be comprised of thousands of components, many of which will be critical to the survival of the crew. And, just like with the car, the habitat will be subject to random failures, as defined by the MTBFs, of all of those components.

If accurate values of MTBF for all of the components could be predicted with limited uncertainty, NASA could understand the potential failure modes of the habitat and could manifest a set of spare components that would cover the potential failures and provide a reasonable level of reliability over the course of the Mars mission. This has been the traditional approach that NASA has applied to the ISS and other human missions.

III. EMAT Capability

NASA performs extensive analysis to assess the reliability of spacecraft. By applying a probabilistic assessment methodology, designers evaluate the likelihood and impact of potential failures and prioritize spares based on those results. To understand the impacts of various sparing approaches and their associated spares mass for EMC missions, NASA has created the Exploration Maintainability Analysis Tool (EMAT). The objective for EMAT is to provide a capability to evaluate the feasibility of different sparing approaches and associated spares mass, and to estimate the contribution to mission safety and mission reliability that will come from modeled systems. EMAT results can be utilized to determine the contribution of the DSH to the probability of loss of crew (PLOC) based on the number of spares manifested on the mission.

A. EMAT Description

EMAT[iii,iv] is a probabilistic simulator of spacecraft system failures and repair activities. A Monte Carlo environment is used to simulate stochastic component failures and repair activities in representative beyond LEO missions. System logic diagrams and spares availability are utilized to evaluate system and mission impacts of failures.

EMAT is structured in several nested layers, each of which executes a different level of analysis. Inputs to the model define system components and operations, element reliability and available spares. System operations are defined through description of the logical relationships between the components in a specific system. A mission is evaluated on a day-by-day basis for a specified mission length, with system failures and repair activities simulated for each day. EMAT monitors two states for each system and its component - whether it is currently functional and/or currently operational. A system or component may be functional (i.e., not in need of repair) but not operational due to component failures elsewhere in the system. Monitoring these two states is necessary since components are less likely to fail while not operating.

The Monte Carlo engine executes a large number of mission simulations (cases), each with independent stochastic failures. The tool monitors statistical convergence of simulation results in order to determine the required number of cases. Finally, a post-processor statistically evaluates the results from Monte Carlo cases to produce probabilistic results.

The model requires several types of input: system descriptions and logic relations, reliability data, repair time, and mission description data. The system descriptions and logic relations define the interdependencies of the system components, which components are removable and replaceable, and which components are consumables with a limited lifetime. The reliability data, including MTBF values, is used to simulate failures of the base components. The spares inventory is a running total of the spares available for the removable and replaceable components. The repair time is used to simulate the repairs of the components that have already failed in the mission simulation. The mission description data includes the mission duration, crew size, and initial states of the components.

EMAT begins a simulation run with no manifested spares and evaluates the overall reliability of the DSH. The tool then assesses the probability of different failure modes and examines each possible spare that could be added, selecting the spare that most effectively reduces risk from a mass perspective. In this manner EMAT produces a curve of overall reliability versus spares mass for the mission.

B. Deep Space Habitat Description

A component-level definition of critical DSH systems has been developed based on input from system experts, International Space Station (ISS) system definition, and spacecraft modeling tools. The model is an initial representative baseline systems definition of a beyond LEO spacecraft. This definition of DSH systems was modeled in EMAT in order to conduct an analysis of maintainability. This model is intended to serve as an initial cut at describing what DSH systems may ultimately look like, as informed by system experts, in order to serve as a starting point to begin conducting sensitivity analysis and trade studies. The actual design of future systems can vary significantly from this description, based on mission requirements, technologies, and constraints.

The baseline system design includes system features, such as redundancy and multiple strings, which are designed into the systems to improve reliability. The model also includes certain limited duration capabilities designed to provide emergency backup to the crew if the primary systems are off-line.

Because the focus of EMAT analysis is on investigating trades between spares mass and mission safety and reliability, the model currently only includes critical systems for which spares are likely to be allocated. Certain systems, such as propulsion, are not currently included because, for this baseline, they are considered to be non-repairable. Other systems are not included because they are considered non-critical, in which a system failure will not lead to loss of mission or loss of crew. These types of systems may be added to future iterations of the DSH model. The systems currently captured in the baseline system definition are: thermal control system, atmosphere control system, attitude and rate determination, command and data handling, communications and tracking, electrical power system, and water recovery and processing system.

IV. Baseline DSH Reliability

Figure 1 shows an example of EMAT output for the DSH systems for a human Mars mission. The results in Figure 1 illustrate the habitat system reliability over the life of a 1,100-day mission versus the associated mass of the manifested inventory of spares. As expected, improving the overall reliability of the system is initially fairly easy to accomplish in an efficient manner. This is achieved because as spares are added that cover high-likelihood, critical failures, the reliability increases fairly rapidly. But, as risk is driven out of the system through the manifesting of critical spares, it becomes increasingly more difficult to make further improvements. This has to do with nature of random failures in complex systems. Once the really likely failures (of which there are few) are protected against, spares are manifested to try to protect against increasingly rare events. There are simply so many potential failure modes, so many critical components, in such a complex machine, that the net product of all these very low probability failures can be very high. So, in order to drive overall reliability to higher and higher levels, one is forced to protect against a huge number of very unlikely failures, resulting in an ever-increasing amount of spares. With the desire to increase crew safety, there is a desire to increase DSH system reliability to even higher levels, resulting in the need to protect against multiple faults in an ever-increasing number of components.

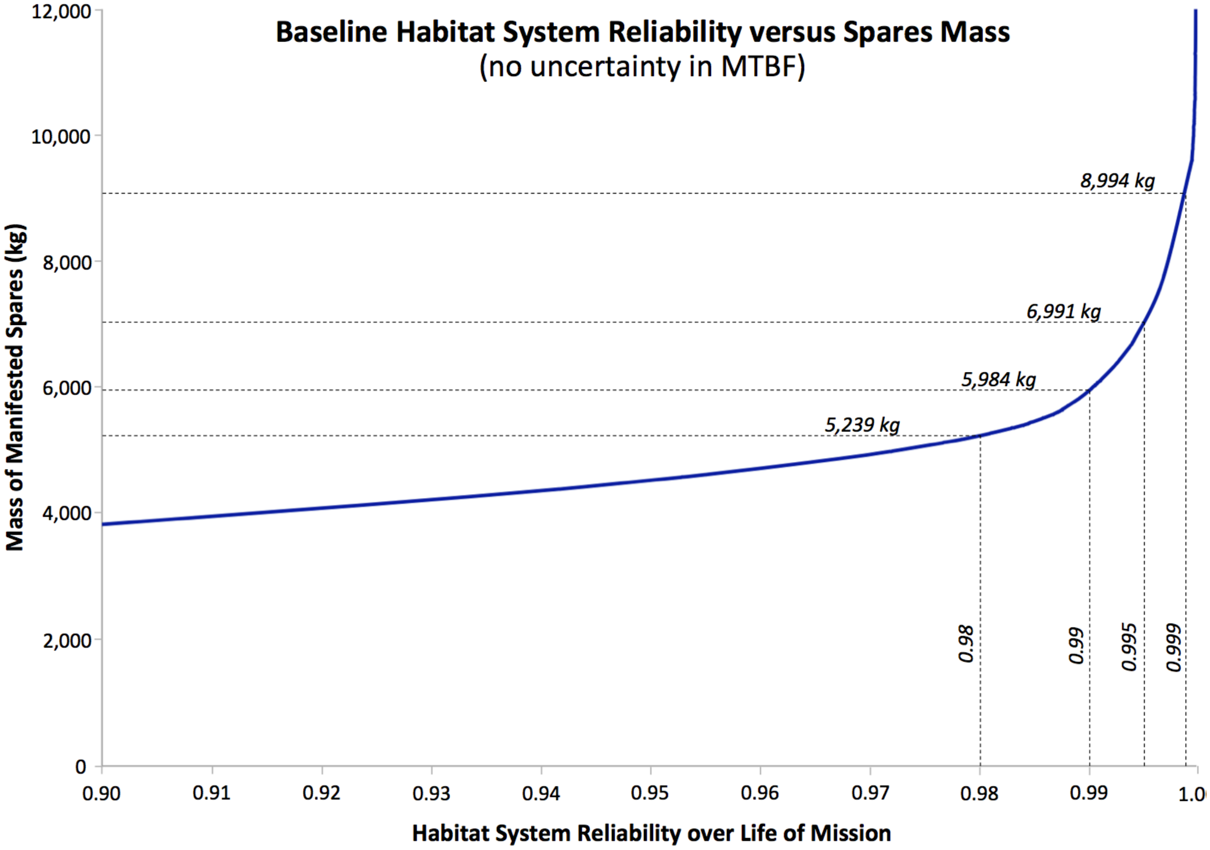

Figure 1- Baseline DSH System Reliability versus Spares Mass (No Uncertainty in MTBF)

While at first look, the total amount of desired mass for DSH spares does not seem inconsistent with current ISS heritage spares needs, implementing these results in terms of architecting a mission to Mars appear to be extremely challenging and potentially very expensive. The results demonstrate that, if spacecraft are designed and maintained in a manner that is similar to what has been done in the past, a large amount of mass and volume will need to be devoted to spares. Because of the high gear ratios, driven by orbital mechanics considerations, involved with reasonable human travel times to Mars, the resultant total launch mass and associated in-space transportation requirements driven by spares needs will be quite large. However, while challenging, it is still feasible that a mission can be designed to accommodate this magnitude of spares.

V. Uncertainty in Component Reliability Data

Unfortunately, as challenging as these results are, they still do not present a sufficiently complete nor accurate story. The results in Figure 1 assume that the system MTBFs, taken from ISS heritage data, represent a perfect state of knowledge of those MTBFs – that the probability that any component will suffer one or more failures over the course of the mission is known precisely. This most certainly will not be the case. The DSH will almost assuredly not be an exact replication of the current ISS habitat module, associated nodes, and external support systems, but will be a new element. And, while many of the DSH systems, to some degree, will likely be similar to systems that have been tested and demonstrated on-board the ISS or some other potential cis-lunar facility, it is highly likely that there will still be a large degree of uncertainty associated with the predicted MTBF values.

The results presented in Figure 1 capture only the aleatoric uncertainty in the DSH system. The manifested spares are intended to reduce the risk of failure due to uncertainty in the operation of the system itself. The uncertainty in the MTBF values themselves represents epistemic uncertainty – uncertainty in understanding of the inherent operational reliability of the system.

This epistemic uncertainty in MTBF estimates will have a drastic effect on the potential overall reliability of the habitat and on the behavior of the relationship between mass and DSH system reliability as demonstrated in Figure 1. As MTBF values vary, the likelihood of component failure and therefore the true potential reliability for the habitat will vary significantly. A notional gross sensitivity of DSH system reliability to MTBF is demonstrated in Figure 2. In this set of results, the baseline current predicted MTBF values used to calculate the results shown in Figure 1, are varied for all critical components. For the red curve, each MTBF value is assumed to be cut in half, increasing the probability of failure. For the green curve, all MTBF values are assumed to be doubled, decreasing the probability of failure. The results from Figure 2 show the sensitivity of the overall reliability to MTBF. Relatively small decreases in MTBF (which can often vary by orders of magnitude) result in substantial changes in overall reliability.

In addition, the results show a significant degree of asymmetry. Reductions in MTBF have a greater relative impact on overall DSH system reliability than do improvements of a similar magnitude. In order to achieve a fixed level of overall reliability, a set of spares has to be manifested that cover anticipated failure modes to a degree that provides that reliability. Improving MTBFs have limited value at that point because there are only small improvements in reliability that are available for each component. In addition, the cost of increasing reliability grows exponentially as MTBF increases[v]. Conversely, as MTBFs decrease, the DSH is no longer adequately protected and the probability of failure for each component increases, driving down overall reliability.

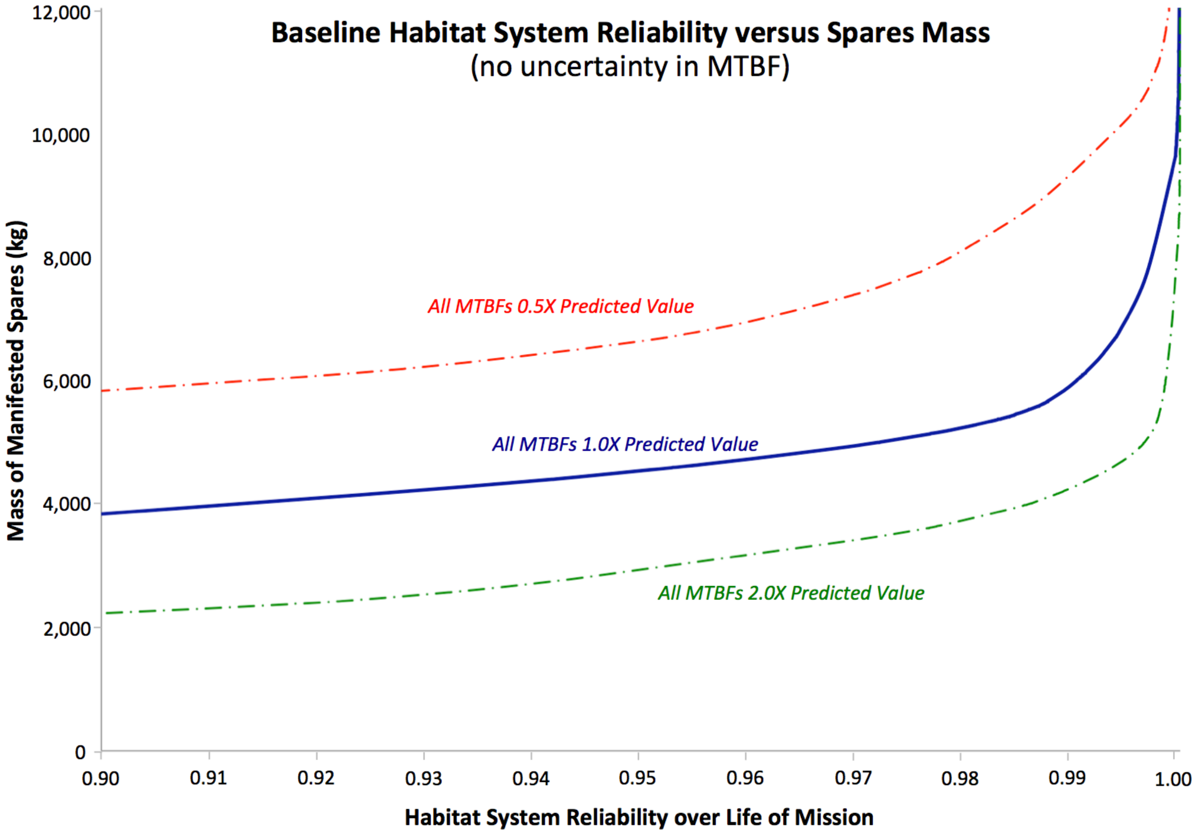

Figure 2 – Sensitivity of DSH System Reliability to Theoretical Variability in MTBF

Again, the examples shown in Figure 2 are notional, derived to demonstrate the sensitivity of reliability to MTBF. As the MTBFs for each and every component will not vary by the same amount or even in the same direction, additional “real-world” information is needed to better understand the likely behavior of future habitat systems. In reality, when uncertainty exists in MTBF values, it is likely that the MTBF values for some components will be higher than initially estimated and some will be lower. The real questions are “what fraction will be higher and what fraction lower?” and “how much will the MTBF values vary?” The answers to these questions will ultimately drive the overall reliability of the DSH.

Luckily, one of the greatest possible resources to explore uncertainty in MTBF value for human spacecraft already exists in the form of the ISS. As currently envisioned, many systems in the DSH will be functionally very similar to those that are currently operating on the ISS. This means that, to some degree, NASA will be able to take advantage of all of the operational experience that is being gained and will be gained in the future on ISS to understand and refine the reliability analysis for future DSH systems.

Table 1 demonstrates the operational experience that has been gained on ISS as it relates to reducing uncertainty in MTBF values[vi]. This table summarizes the operational time versus the initially predicted MTBF for the most vital (all Criticality Level 1 and Criticality Level 2 spares) ISS components on-board the habitable portion of the non-Russian side of the ISS, the United States Operational Segment (USOS). These components roughly represent those that would be critical to crew survival in the DSH. This dataset will most closely represent that which will be used for DSH reliability analysis.

Table 1 – Operational Times Versus MTBF
(for U.S. Criticality Level 1 & Criticality Level 2 Components)

Accumulated Op. Time / MTBF	Fraction of Components Today	Fraction of Components Through 2028 (est.)
<0.1	24.8%	19.4%
0.1 - 0.5	29.5%	11.2%
0.5 - 1.0	29.9%	17.3%
>1.0	15.8%	52.1%

The amount of operational experience varies significantly between components. This is because the range of predicted MTBFs varies substantially between individual components (from a low of about 2,000 hours to a high of 100 Million+ hours). Also, the amount of accumulated operational time varies between components. For certain components, of which there are multiple copies on ISS, the operational times of all active components can be summed together, resulting in a greater equivalent overall lifetime. For others, of which there are only single copies that run only periodically, the operational lifetimes have been quite small.

The second column in Table 1 shows the percentage of components that have accumulated certain levels of operational experience through June of 2016. Approximately 25% of these components have not yet achieved a tenth MTBF (0.1X MTBF) of their operational experience. Another 30% have accumulated operational lifetimes between a tenth and half (0.1X and 0.5X) MTBF. 30% have accumulated operational lifetimes of between a half and one (0.5X and 1.0X) MTBF. Only 15% have lifetimes greater than 1.0X MTBF.

Typically, in order to gain a high level of confidence that an actual MTBF is reasonably close to the predicted operational time, very long accumulated operational times are required. To have a confidence level of 95% in the MTBF value, an operational period on the order of three times the MTBF (3X) is required. To increase the confidence to 99%, a period approaching five times the MTBF (5X) is required. These long periods are required to increase confidence because the MTBF estimates are simply an average time to occurrence of an anticipated failure. It is the nature of random failures that sometimes failures can occur early (unlucky) and sometime they can occur late (lucky). Very long operational periods are required to really understand the average frequency that failures will occur. However, even with accumulated operational lifetimes that are significantly lower than the 3X to 5X MTBF described, it is possible to begin to reduce uncertainty in MTBF and to refine MTBF estimates.

The ISS Program is diligent about tracking repair activities, evaluating failure data, and using that information to better understand MTBF estimates for all components. Typically, MTBF estimates will be evaluated and potentially updated for components that have achieved 0.5X of the initial MTBF estimate or which have experienced failures. The reanalysis of ISS component MTBF is performed using a Bayesian process to evaluate observed reliability. The methodology employed by the ISS Program is described in detail by Anderson et. al[vii].

By applying this process, the ISS Program has modified the MTBFs of approximately 55% of the Criticality 1 (Crit. 1) and Criticality 2 (Crit. 2) components, through June 2016. The fact that MTBF values have been updated for a number of ISS components does NOT indicate that there is no longer any uncertainty in the MTBF estimates, but rather that there is enough operational experience to begin to reduce that uncertainty.

The third column in Table 1 indicates the expected level of operational experience that would be gained, if the ISS were to operate through 2028. This data was derived by extrapolating the accumulated operational time for each component through 2028, based on the level of experience gained from initial operations through 2016. By 2028, it is expected that there will be a significant percentage of components that still will not have achieved the 0.5X MTBF threshold (approximately 30%). However, 17% of components will have operational lifetimes of between 0.5X and 1.0X MTBF and 52% greater than 1.0X MTBF. This additional experience will allow the program to develop modified MTBF estimates for up to an estimated 88% of all Crit. 1 and Crit. 2 components. This represents a significant increase in overall operational experience and will help reduce the uncertainty regarding MTBF estimates for ISS components.

VI. Variability in ISS MTBF Estimates

The component reliability data collected on ISS can be used not only to update MTBF estimates but can also be evaluated to begin to define a distribution of updated MTBF values versus initial MTBF estimates. Because a significant fraction of critical ISS components have been evaluated and have had MTBF estimates modified based on operational experience, it is possible to evaluate how MTBF values have changed over time, in order to predict what the variability in MTBF *may be* in the future. For all components in the subject data set that have had the MTBF value (associated with random and induced failures only) modified, a ratio of the modified estimate to the initial estimate was calculated. These estimates were then statistically evaluated to determine the distribution of this ratio across all components. Figure 3 illustrates the results of this analysis. The data in Figure 3 is presented as a cumulative distribution. The horizontal axis indicates the ratio of modified MTBF values to initial values. The vertical axis indicates the total fraction of components that exceed that ratio.

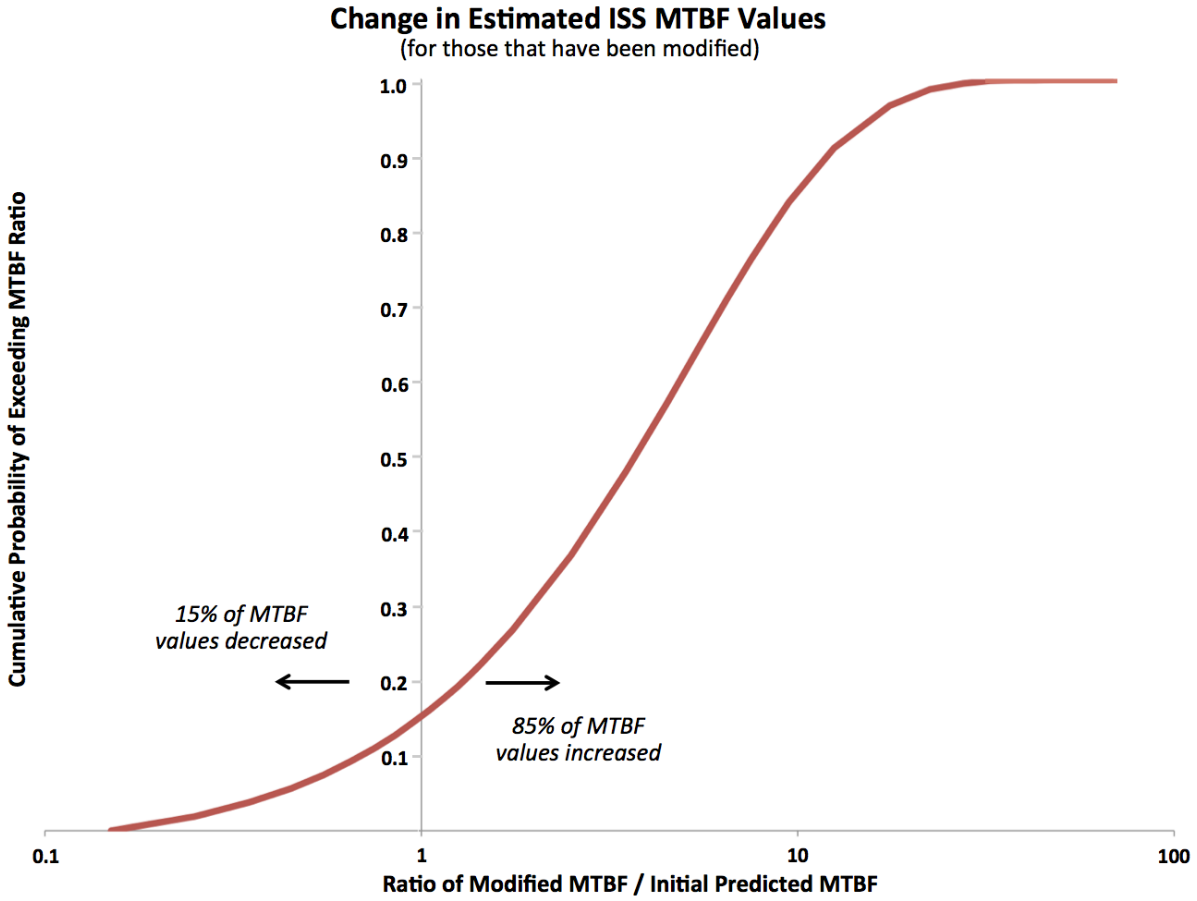

Figure 3 – Change in Estimated MTBF Values (for those that have been modified)

The results shown in Figure 3 indicate that approximately 15% of ISS components have seen a decrease in MTBF value (i.e. have an MTBF ratio of less than 1.0) – indicating that the reliability of the component was less than initially predicted. Of the components that saw a decrease in MTBF, a very small fraction of ISS components saw a substantial decrease; approximately 3% had an MTBF ratio of 0.25 or lower. Figure 3 also shows that approximately 85% of components experienced an increase in MTBF value. Of those that improved, approximately 14% had an MTBF ratio of at least 10.0.

The curve shown in Figure 3 is by no means an exact prediction on future variability in ISS component MTBFs. There is certainly no expectation that the updated MTBF values for components, derived from ISS experience, are fully correct and, as discussed, many of them are still based on limited operational experience. However, because the modified estimates are all based on some level of operational ISS experience, it is likely that the distribution across all relevant components of how MTBF values have changed is at least somewhat representative of the relationship between actual MTBF values and initially predicted values. The distribution represented in Figure 3 was re-derived for various sub-sets of the initial component data set, filtering by type of component, magnitude of the initial MTBF estimate, and level of accumulated operational life. In each case, the derived distribution was similar in nature to that shown in Figure 3. This similarity indicates that the distribution should be at least representative of the relationship between actual MTBF and initially predicted MTBF.

The operational experience gained on ISS will, to some degree, allow NASA to reduce the uncertainty associated with MTBF values for future DSH systems. The degree to which this experience will be applicable is also somewhat uncertain however. The ISS was largely designed and constructed in the 1980s to 1990s. The DSH is expected to be designed and built in the late 2020s. It is almost certain that this 30 to 40-year difference will lead to changes in the design and manufacturing of systems and components. As new technologies and materials become available, there will be a strong desire to incorporate these capabilities into the DSH in order to improve performance, reduce mass, and even to improve reliability. It is also likely that components, even those that are nominally similar to ones on ISS, will because of vendor availability and programmatic reasons have to be acquired from different manufactures and different production facilities. Additionally, systems will have to be reconfigured and rearranged in order to be packaged in the DSH. It is unlikely that DSH systems will be housed in ISPRs (International Standard Payload Racks), as many are in the ISS. Rearranging systems will lead to changes in pipe and cable runs, and changes in thermal, power, and vibrational profiles. Finally, the environment that the spacecraft will operate in will also change significantly. In particular, the radiation environment of the DSH will be much different from what is experienced on ISS. All of these factors may contribute to further uncertainty in MTBF values and may, to some degree, reduce the value of the experience gained on ISS. Unfortunately, the degree that these changing conditions will impact MTBF values is unknown. Therefore, the actual level of uncertainty in MTBF values for the DSH is also unknown at this time and for the foreseeable future.

It is possible, however, to set reasonable bounds on possible MTBF uncertainty for the DSH. The authors derived two cases to represent these bounds:

- **High Uncertainty Case** – In the most conservative case, the assumption was made that none of the accumulated ISS experience will be applicable to predicting MTBF for components in the DSH. For this case, the MTBF uncertainty defined in Figure 3, will be applicable to *all* components in the modeled DSH systems.
- **Low Uncertainty Case** – In the most optimistic case, the assumption is made that all of the knowledge gained on ISS will be directly applicable to the DSH. The environmental factors that are described above will have only minor impacts on MTBF values and uncertainty will be reduced based on actual operational experience.

The actual level of MTBF uncertainty will likely fall somewhere between these two extremes. Investigating these two cases therefore will at least provide a range of where the ultimate DSH system reliability may fall, when accounting for MTBF uncertainty.

To explore the impacts of component MTBF uncertainty on overall DSH reliability, the authors developed a Monte Carlo extension to the EMAT analysis tool. In this extension, rather than executing a single run of EMAT utilizing fixed MTBF values, numerous runs were completed with the MTBF for each component in the DSH model being allowed to vary according to a predefined distribution. These updated MTBF values were used in EMAT to determine the resultant overall reliability as a function of spares mass for the mission for that run. This process was repeated over thousands of runs, with the MTBFs varying independently for each run. The data was then statistically evaluated over all of the Monte Carlo runs to determine the resultant levels of overall reliability that would be achieved with varying confidence levels.

The entire process was repeated for different sets of spares inventories, representing different spares mass, taken from the deterministic data set (with no MTBF uncertainty). The data was then statistically evaluated over all of the Monte Carlo runs to determine the resultant level of achieved reliability as a function of spares mass at different levels of confidence.

The Monte Carlo based MTBF uncertainty tool was then used to evaluate each of the two bounding cases for MTBF uncertainty. By selectively applying the uncertainty distribution shown in Figure 3 to different components, it is possible to simulate each of these cases. For the ‘High Uncertainty’ case, in which full MTBF uncertainty is assumed, the distribution was applied to every component, allowing the MTBF values to vary over the full range of the distribution. For this case, every component was sampled for every run, producing an updated “actual” MTBF value.

For the ‘Low Uncertainty’ case, a similar process was followed; however, the degree of uncertainty applied to each component varied, based on the level of operational experience that is anticipated to be gained on ISS. The data for component accumulated operational time, projected through 2028, was used to scale the level of deviation in

MTBF. For all components that will not have achieved at least 0.5X MTBF by 2028, the full uncertainty represented in the distribution from Figure 3 was applied. For any component where the operational experience was greater than or equal to 3X, no uncertainty was applied and the initial MTBF estimate was used. For all other components, the distribution in Figure 3 was sampled to develop a maximum MTBF deviation for each component. That deviation was then scaled linearly based on level of operational experience, with the full uncertainty applied as MTBF approached 0.5X and the uncertainty going to zero as operational experience approached 3.0X. The Monte Carlo cases were then executed and processed in a manner identical to that described for the 'High Uncertainty' case.

The results of the uncertainty analysis for the 'High Uncertainty' case are presented in Figure 4. The results for the 'Low Uncertainty' case are presented in Figure 5. For these plots, the horizontal axis, representing the Overall DSH System Reliability is plotted on an inverse logarithmic scale. This is done to facilitate the assessment of the results at high levels of reliability, similar to what will be required for actual missions. Each figure shows the initial, deterministic results as a solid blue line. The 5th, 25th, 50th, 75th, and 95th percentile confidence intervals are shown as dashed lines. These lines represent the likelihood that a certain level of reliability could be reached, given the uncertainty in MTBF values.

What is immediately obvious from Figures 4 and 5 is that the epistemic uncertainty in MTBF has a major impact on DSH system reliability. If the two limiting cases represent a band of possible future behavior, then it is apparent that the overall reliability of the DSH will be significantly lower than has been predicted based on known MTBFs.

Using the deterministic point value, with no MTBF uncertainty, the set of spares that is manifested to provide a 0.99 DSH reliability for the Mars mission, results in 5,984kg of manifested spares. In the best-case "low uncertainty" case, shown in Figure 5, at a 50th percentile confidence level, the reliability remains at approximately 0.99. However, at a 75th percentile confidence level to the reliability drops to 0.98 and at a 95th percentile confidence it drops to 0.92. In the worst-case "high uncertainty" case, shown in Figure 4, at a 50th percentile confidence level, the reliability drops to 0.91. At a 75th percentile confidence level, the reliability drops to 0.83 and at a 95th percentile confidence it drops as low as 0.63.

Because the level of actual uncertainty will fall between these two bounding cases, it will be necessary to manifest additional spares in order to achieve an acceptable level of system reliability. The added spares that would be required to increase overall DSH reliability to the initially desired level would require a large mass and volume increase, if possible at all. Even under the "Low Uncertainty" scenario, the spares mass required to achieve the initially desired 0.99 reliability at 95th percentile confidence would be over 12,000kg of spares. For the "High Uncertainty" scenario, it would require over 17,000kg of spares to achieve similar levels of reliability and confidence.

As initially discussed above, the primary reason behind the dramatic reduction in reliability due to MTBF uncertainty has to do with asymmetric behavior of the system and spares. Using the distribution of modified MTBFs, defined in Figure 3, roughly 85% of the components in the DSH will actually end up with a longer (better) MTBF in each Monte Carlo run. Only 15% will end with shorter MTBF values. Even among those components that have a worse MTBF value, only a very small portion will be significantly worse (particularly in the Low Uncertainty case). However, it is this very small number of critical components that drive the behavior and reliability of the entire system. The components that end up with improved MTBF values do not contribute much in the way of improving overall reliability (again, because sufficient spares have already been manifested to protect against those failures). For those that have significantly worse MTBFs, those failures have not been adequately protected against and result in much lower DSH reliability. Because of the nature of the uncertainty in MTBF, there is no way to know for sure which specific components will end up with lower than expected MTBFs, so a larger than desired number of components will need to be manifested to account for and mitigate this uncertainty.

While at a minimum the doubling of the needed spares mass (best case) may not seem insurmountable to provide from DSH perspective, this only represents a fraction of the true overall exploration architecture level "cost". To accommodate this increased spares mass additional pressurized mass and volume and/or conditioned external mass and volume will be required. This will necessitate a dramatic increase in the required transportation system capability needed to move this increased mass and volume round trip from Earth to Mars with an associated substantial increase in Earth-to-Orbit (ETO) cargo delivery capability. Finally, the uncertainty in the DSH system MTBFs due to random failures is not the only source of epistemic uncertainty. Other sources of epistemic uncertainty associated with induced failures, design and manufacturing failure rate uncertainties, and modeling uncertainties may contribute an equivalent amount of growth in required spares mass. The result is that it may not be possible to develop a DSH that has a sufficient level of reliability to support human missions to Mars, if NASA continues to use current approaches for maintainability. The cost in terms of both required transportation system performance and the cost of needed spares sufficient to keep the system functioning with a very high degree of reliability required for the mission most likely will be prohibitive.

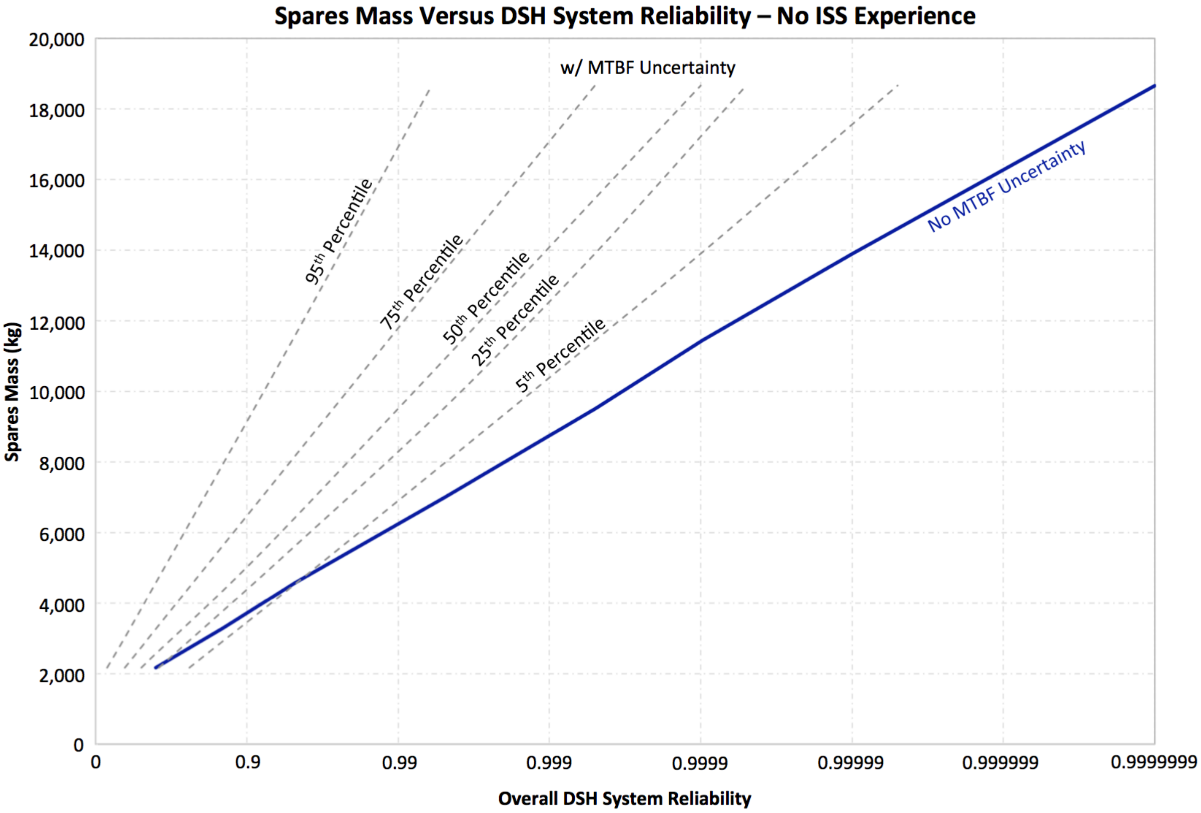

Figure 4 – 'High Uncertainty' Case – Spares Mass versus DSH System Reliability

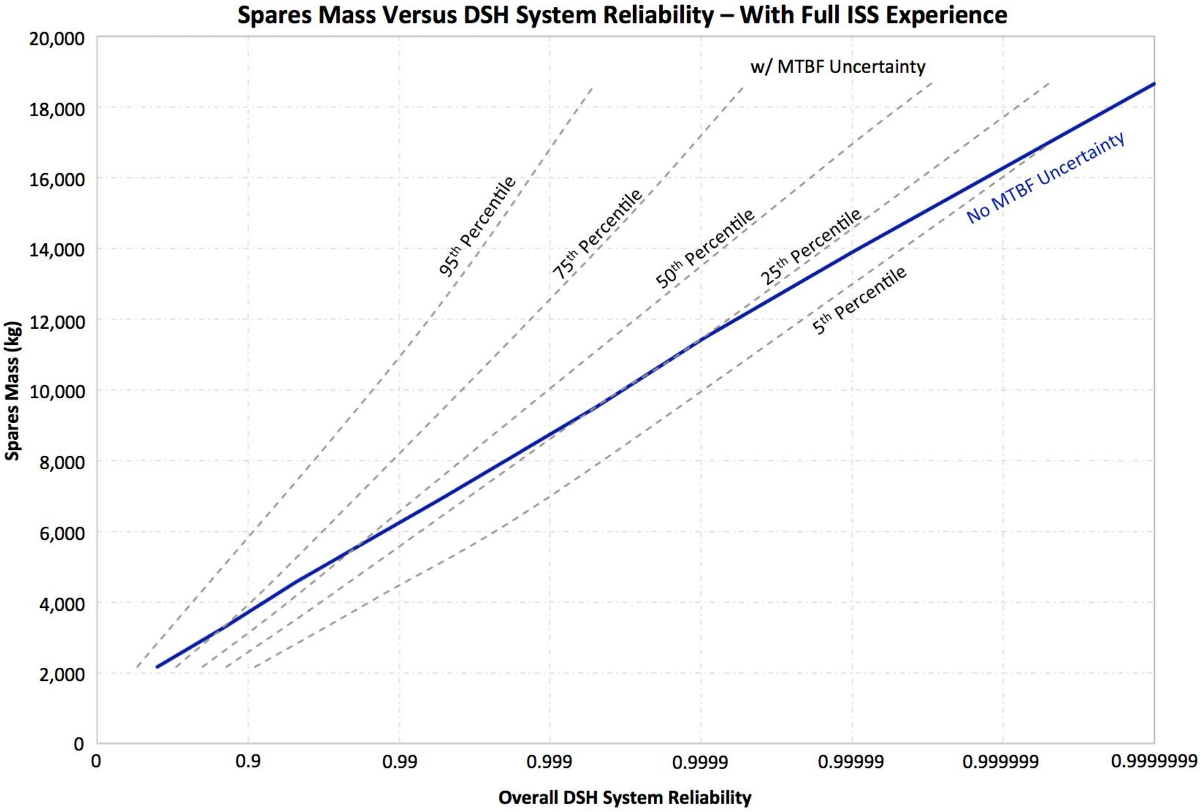

Figure 5 – 'Low Uncertainty' Case – Spares Mass versus DSH System Reliability

VII. Options to Improve System Reliability

Given that manifesting tens of thousands of kilograms of spares, and the associated transportation system requirements, in order to achieve an acceptable level of reliability will be extremely challenging from a mission architecture standpoint, NASA will need to consider other options to improve overall reliability.

Plan Probabilistically: The first option is perhaps the most obvious. Rather than selecting spares deterministically, assuming fixed MTBF values, planners should include the level of uncertainty in each MTBF value in the sparing analysis. Including uncertainty will prioritize the inclusion of spares for components that have a large degree on uncertainty and, as a result, contribute most heavily to reduction in probabilistic reliability.

Consideration of Modification to Systems: As discussed, there will likely be a desire to update and improve ISS heritage systems for the DSH. This will be done for primarily performance and mass reasons but may also be done to improve the reliability itself. As modifications are made, they will, to some degree, invalidate the reliability experience that has been accumulated on ISS. This analysis has shown that added uncertainty has a negative impact on net achieved reliability. Any changes proposed to existing ISS systems that will be planned for use in future DSH systems or the use of totally new systems with limited operational lifetimes should be carefully considered, balancing the potential gain with the potential increase in uncertainty in MTBF and the resultant decrease in overall system reliability.

Change the approach to maintenance and repair: The large required mass and associated volume to accommodate spares is largely driven by the overall approach to maintainability, which is focused on manifesting of spare parts to allow for repair of failed systems and components. Emerging technologies, such as in-space manufacturing (ISM), present other potentially attractive options for enabling a high level of supportability[viii]. If a fraction of required spares could be manufactured on-board the spacecraft during the mission, utilizing common equipment and stock, it may be possible to achieve high levels of reliability at a significantly reduced mass. ISM largely invalidates the issues with MTBF uncertainty, as relevant components can be manufactures on-demand as actual random failures occur. However, additional study is required to evaluate the applicability of technologies such as ISM to different DSH components and to determine the impacts of allowing in-space manufactured spares to be used on these systems. To fully achieve the potential value/return on investment of this type of approach, the following additional factor may need to be accomplished in parallel.

Reduce System Complexity: Certain systems are incorporated into the DSH to reduce consumables mass for the crew. These systems, which are designed to recycle air and water, contain a significant fraction of the overall number of critical components. For these systems, there is an upper limit of required spares mass where it will still make sense to continue to include the system in a future DSH design. For example, rather than manifesting a more closed-loop system (e.g., water, air, waste, etc.) and all of the required spares, it will be more efficient (and likely less risky) to simply manifest the consumables themselves. Decisions such as these must be made in consideration of the inherent uncertainty in reliability.

VIII. Conclusion & Forward Work

The analyses executed for this paper were intended to show the impact of one specific type of epistemic uncertainty on overall DSH system reliability, concentrating on one critical factor – random failures as represented by MTBF. This is by no means a complete analysis of the uncertainties involved in reliability analysis. There are numerous other factors that may contribute to reliability and will also have to be evaluated and considered.

Uncertainty in element lifetime, which define failures due to component wear-out can also be uncertain, and will have to be protected against. Similarly, another parameter that relates to MTBF, the K-Factor, defines the probability of "induced failures" in spacecraft components and systems. Similar to MTBF values, component K-Factors are defined based on past experience and may also involve a high degree of uncertainty for deep-space missions.

Finally, there is the issue of "design and manufacturer errors". A significant fraction of failures on-board ISS have been attributed to "other" causes, including some number associated with deficiencies in design or manufacture of components. The root causes of these failures have been diagnosed and rectified, therefore from an ISS reliability modeling perspective they have not been included in the Bayesian analysis to update ISS MTBF values and subsequently do not contribute to overall probability of future failure for those ISS components. However, for a deep-space mission, these "other" failure drivers, including design and/or manufacturing errors, will likely also be an issue and will need to be accounted for and better characterized to understand their impact in the future exploration architecture DSH design process. Because many components will not be identical to those used and operated on ISS there may be new sources of design and manufacturer errors. It is unlikely that most of these errors will be discovered during the limited test period anticipated for the DSH. Additional failures, beyond those predicted by component lifetime, MTBF, and K-Factor, may then occur during the mission, further reducing reliability.

The analyses described in this paper demonstrate that uncertainty in reliability will be a major contributor to achieving a desired level of mission safety and assurance. In order to develop an overall approach to designing and maintaining the systems that will take humans to and from Mars and on the Martian surface, it is critical that NASA and others continue to evaluate data from ISS and other sources to better predict and account for uncertainty in reliability analysis. As part of this effort, NASA must continue to collect and analyze ISS data and should begin to investigate the applicability of that ISS experience to future deep space vehicles. One potential additional source of extremely valuable heritage information would be the inclusion of maintenance and system data from the series of long duration Russian human-rated spacecraft (ISS Russian Segment, Mir, and Salyut).

Recognizing that the ability to reduce uncertainty in reliability estimates for DSVs may be limited, NASA must also begin to evaluate alternate strategies to maintaining and repairing future spacecraft. Consideration of reliability and uncertainty in system design will be critical, as will the incorporation of new technologies, such as ISM, to help solve maintainability issues.

Acknowledgments

The authors would like to acknowledge NASA's Human Exploration and Operations Mission Directorate (HEOMD) Advanced Exploration Systems (AES) Division as the providers of funding for this analysis through the Evolvable Mars Campaign study. In addition, this research was supported by a NASA Space Technology Research Fellowship (grant number NNX14AM42H).

References

[i] https://www.nasa.gov/content/spaceflight-architecture, accessed July 29, 2016

[ii] J.D. Power 2013 U.S. Initial Quality Study$^{\text{SM}}$

[iii] Stromgren, C., Terry, M., Cirillo, W., Goodliff, K. and Maxwell, A., "Design and Application of the Exploration Maintainability Analysis Tool," AIAA Space 2012 Conference and Exposition, AIAA-2012-5323, Pasadena, CA, September 2012.

[iv] Stromgren, C., Terry, M., Mattfeld, B., Cirillo, W., Goodliff, K., Shyface, H., and Maxwell, A., "Assessment of Maintainability for Future Human Asteroid and Mars Missions," 2013 AIAA Space Conference & Exposition, AIAA- 2013-5328, San Diego, CA, September 2013.

[v] Owens, A., and De Weck, O., "Limitations of Reliability for Long-Endurance Human Spaceflight", 2016 AIAA Space Conference & Exposition, Long Beach, CA, September 2016.

[vi] International Space Station Safety & Mission Assurance Office's Maintenance & Analysis Data Set (MADS) - limited access database

[vii] Anderson, L., Carter-Journet, K., Box, N., DiFilippo, D., Harrington, S., Jackson, D., Lutomski, M., "Challenges of Sustaining the International Space Station through 2020 and Beyond: Including Epistemic Uncertainty in Reassessing Confidence Targets," AIAA Space 2012 Conference and Exposition, AIAA-2012-5320, Pasadena, CA, September 2012.

[viii] Owens, Andrew C. and de Weck, Oliver L., "Systems Analysis of In-Space Manufacturing Applications for the International Space Station and the Evolvable Mars Campaign," 2016 AIAA Space Conference & Exposition, Long Beach, CA, September 2016.