

# Limitations of Reliability for Long-Endurance Human Spaceflight

Andrew C. Owens\* and Olivier L. de Weck†

*Massachusetts Institute of Technology, Cambridge, MA 02139, USA*

Long-endurance human spaceflight – such as missions to Mars or its moons – will present a never-before-seen maintenance logistics challenge. Crews will be in space for longer and be farther way from Earth than ever before. Resupply and abort options will be heavily constrained, and will have timescales much longer than current and past experience. Spare parts and/or redundant systems will have to be included to reduce risk. However, the high cost of transportation means that this risk reduction must be achieved while also minimizing mass. The concept of increasing system and component reliability is commonly discussed as a means to reduce risk and mass by reducing the probability that components will fail during a mission. While increased reliability can reduce maintenance logistics mass requirements, the rate of mass reduction decreases over time. In addition, reliability growth requires increased test time and cost. This paper assesses trends in test time requirements, cost, and maintenance logistics mass savings as a function of increase in Mean Time Between Failures (MTBF) for some or all of the components in a system. In general, reliability growth results in superlinear growth in test time requirements, exponential growth in cost, and sublinear benefits (in terms of logistics mass saved). These trends indicate that it is unlikely that reliability growth alone will be a cost-effective approach to maintenance logistics mass reduction and risk mitigation for long-endurance missions. This paper discusses these trends as well as other options to reduce logistics mass such as direct reduction of part mass, commonality, or In-Space Manufacturing (ISM). Overall, it is likely that some combination of all available options – including reliability growth – will be required to reduce mass and mitigate risk for future deep space missions.

## Nomenclature

$\alpha$	Reliability growth rate
$\beta$	Logistics mass savings growth rate (representative)
$\gamma$	Reliability growth function scale parameter
$\lambda$	Failure rate
$\rho(t)$	Instantaneous failure rate at time $t$
$c$	Cost
$C(t)$	Cumulative average failure rate at time $t$
$f$	Feasibility of increasing reliability
$\overline{FEF}$	Mean Fix Effectiveness Factor
$MTBF_G$	Goal Mean Time Between Failures
$MTBF_{GP}$	Reliability growth potential
$\eta$	Multiplier on Mean Time Between Failures
$\hat{n}$	Number of spares or redundant items provided

---

\*Ph.D. Candidate and NASA Space Technology Research Fellow, Department of Aeronautics and Astronautics, 77 Massachusetts Ave. Bldg. 33-409, AIAA Student Member.

†Professor of Aeronautics and Astronautics and Engineering Systems, Department of Aeronautics and Astronautics, 77 Massachusetts Ave. Bldg. 33-410, AIAA Associate Fellow.

$n$	Total number of items provided (initial plus spares)
$N(t)$	Number of failures observed up to time $t$
$R(t)$	Reliability at time $t$
$R_{max}$	Maximum achievable reliability
$R_{min}$	Initial/Minimum reliability
$t$	Time
AES	Advanced Exploration Systems
AMSAA	Army Materiel Systems Analysis Activity
CDF	Cumulative Distribution Function
DoD	Department of Defense
DSH	Deep Space Habitat
ECLS	Environmental Control and Life Support
EMC	Evolvable Mars Campaign
FEF	Fix Effectiveness Factor
HEOMD	Human Exploration and Operations Mission Directorate
ISM	In-Space Manufacturing
ISRU	In-Situ Resource Utilization
ISS	International Space Station
LEO	Low Earth Orbit
MS	Management Strategy
MTBF	Mean Time Between Failures
NHPP	Non-Homogeneous Poisson Process
ORU	Orbital Replacement Unit
P(LoC)	Probability of Loss of Crew
POS	Probability of Sufficiency

## I. Introduction

FUTURE missions beyond Low Earth Orbit (LEO) will see humans go farther from home than ever before, and stay in space for a significantly longer amount of time. These missions will have severe constraints on resupply or abort options, and in some cases crews may not have an option for a timely abort back to Earth in the case of an emergency. As a result of these constraints, the criticality of maintenance capability is increased, since a failure that might provide enough time to return to Earth in a LEO mission context could prove catastrophic if no return is possible. Therefore, mission planning and system design must provide a very high probability that required spacecraft functions will be available for the full duration of the mission. This availability may be achieved through several means, including systems composed of highly reliable components, added redundancy, design for maintainability, or contingency options. Given the high cost associated with transporting materials from Earth to destinations beyond LEO, this high level of confidence must be achieved while minimizing the total mass of the system.<sup>1-4</sup>

The concept of increasing the reliability of systems is commonly discussed as a means to reduce risk and mass by decreasing the probability that components or subsystems will fail during a mission and therefore reducing the number of redundant elements or spare parts that need to be carried in order to achieve a desired probability of success.<sup>3</sup> While increased reliability can have a positive impact on the supportability of a mission, the scale of reliability growth required for long-duration missions can be extreme, and increases exponentially as higher levels of mission confidence are desired. For repairable systems, the reduction in spares mass achieved as a function of increased reliability has diminishing returns, and is small if only a subset of components is affected. In addition, the cost of increasing reliability grows exponentially, and significant test and operations time may be required to verify high reliability.<sup>5-7</sup> As a result, high reliability systems may be very expensive to achieve (both in terms of financial cost and development time) and reliability alone may not be a cost-effective means to achieve high confidence in long-duration systems.<sup>7,8</sup>

This paper presents a sensitivity analysis of the risk and logistics mass associated with Deep Space Habi-

tat (DSH) critical systems for a Mars transit mission. Section II presents background and definitions for reliability and endurance and discusses the maintenance logistics challenges of long-endurance human spaceflight. Section III examines the relationship between cost, test time, and component reliability, discussing various models and examining trends. Section IV examines the benefits of increased reliability in terms of maintenance logistics mass reduction. Section V discusses these results; potential alternative approaches to system supportability that may provide more robust systems – such as commonality, In-Space Manufacturing (ISM), and lower level repair – are discussed along with the implications of these results with regard to system design for long-endurance missions. Finally, section VI presents conclusions.

## II. Reliability Challenges for Long-Endurance Missions

### A. Background and Definitions

#### 1. Reliability

Reliability is defined as the probability that an item will perform its intended function for a given period of time under a given set of operating conditions.<sup>6</sup> Reliability for a particular item is often characterized using the constant failure rate model, which assumes that failures are stochastic events that occur at some constant rate, known as the failure rate,  $\lambda$ .<sup>9</sup> The inverse of failure rate is Mean Time Between Failures (MTBF), or the average amount of time between failure events. Importantly, failure rate and MTBF for a particular item are parameters that describe a random variable – the amount of time that the item will function – and are not parameters that can be used deterministically to determine how many times an item will fail. In the constant failure rate model, the time to failure is characterized by an exponential distribution, and the reliability  $R(t)$  (i.e. the probability that an item with failure rate  $\lambda$  will still be functional after some time  $t$ ) is the complement of the exponential Cumulative Distribution Function (CDF):

$$R(t) = e^{-\lambda t} = e^{-\frac{t}{MTBF}} \quad (1)$$

Equation 1 illustrates the pitfalls of using MTBF as a deterministic parameter: if MTBF is equal to the mission time  $t$ , the probability that the item will still be functioning is just under 0.37. In order to achieve a high probability that an item will not fail over a given amount of time, the MTBF for that item must be significantly greater than the operating time period.

When multiple failure and repair or switchover events are considered (i.e. if the system includes redundancy or spare parts), the probability that a given number of failures will be experienced is given by the CDF of the Poisson distribution, which models the number of times a random event with a constant rate will occur within a given time period.<sup>10</sup> For allocation of spare parts or redundant units to account for potential failures, a key metric here is Probability of Sufficiency (POS), or the probability that the number of replacement items provided is greater than the number of failures that will occur.<sup>11</sup> When items fail at a constant rate, POS is given by the CDF of the Poisson distribution:<sup>11</sup>

$$POS(n, t) = \sum_{k=0}^{\hat{n}} e^{-\lambda t} \frac{(\lambda t)^k}{k!} \quad (2)$$

where  $\hat{n}$  is the number of spares (or off line redundant items) provided. This is one less than the total number of items provided,  $n$ , which includes the initially installed item. Equations 1 and 2 can be used to assess the reliability of an item (or system of items) with a given failure rate or MTBF over a given period of time.

#### 2. Endurance

One of the most commonly used descriptor for the amount of time associated with a given mission is duration, which refers to the time between the start and end of the mission. However, it is important to distinguish between duration and endurance, which is defined as the amount of time that a system must function without resupply.<sup>12</sup> When a mission has no resupply, duration and endurance are equivalent. This has been the case with most human spaceflight experience (e.g. Apollo, Shuttle). However, when periodic resupply is available the endurance of a mission may be significantly shorter than its duration. This is the

case with the International Space Station (ISS) – even though humans have continuously occupied the station for more than a decade and a half, the ISS is resupplied from the ground approximately every 3 months. As a result, while the ISS is a long-duration human spaceflight system, it is not a long-endurance system. No human spaceflight experience has been gained on the endurances required for a mission to Mars and back.

This distinction is important for maintenance forecasting, since mission endurance represents the planning horizon that reliability, maintenance logistics, and risk must be assessed over. This is particularly important when no quick abort options will be available, as is the case for missions to Mars. Under these conditions, a system failure that cannot be repaired could result in loss of function that leads to loss of crew; therefore, the maintenance logistics provided and system reliability achieved are direct contributors to Probability of Loss of Crew (P(LoC)). More precisely, the overall POS for critical systems – a function of the number of spares or level of redundancy provided and the failure rate or MTBF achieved for each item – provides a bound on the achievable P(LoC) for a given mission, which can be thought of as the maintenance logistics contribution to P(LoC).<sup>13,14</sup> While reliability calculations involving duration are important for system operations planning even when resupply is available, when examining the risk of insufficient spares as it pertains to P(LoC).

## B. Reliability and Risk for Deep Space

Future crewed exploration missions will be a reliability challenge unlike any previous human spaceflight experience. Past experience – including expeditions to the moon and back during Apollo, orbital sorties in the Space Shuttle, and sustained operations in LEO on the ISS – has consisted entirely of short-endurance missions. Crews have always had the option to abort and return to Earth within a few days at most, and long-duration operations have been supported by resupply flights every few months. As a result, past missions have been able to reduce risks with an Earth-dependent support structure. This option will not be available for future missions, which will take humans farther from Earth than ever before, beyond the reach of timely abort or resupply options in the event of an emergency. In addition, these missions will have endurances significantly longer than previous experience. For example, the Evolvable Mars Campaign (EMC) DSH must be designed to support the crew for 1,100 days in deep space on a Mars transit mission (round trip, including time in Mars orbit as a safe haven);<sup>15</sup> this is an endurance approximately 12 times longer than the typical resupply interval for the ISS. New approaches must be developed and implemented to mitigate risk and enable Earth-independent human spaceflight.<sup>1-4</sup>

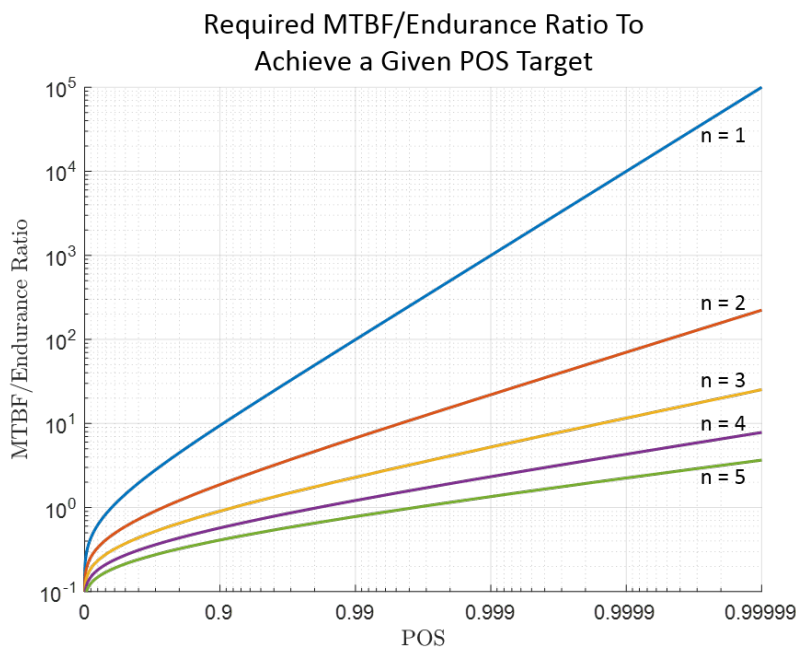


Figure 1. Ratio of MTBF to mission endurance required to achieve a given POS, for a total number of units  $n$  ranging from 1 (i.e. single string) to 5 (i.e. 4 standby redundant units in addition to the initial unit). Note that both the x- and y-axes are plotted on a logarithmic scale. These results assume that all repairs are completed successfully and there are no manufacturing defects, environmental effects, or unanticipated interactions.

Table 1. MTBF required to reduce probability of failure to less than 1 in 1000 with a given number of units, both as a ratio to endurance and as the value required for a 1,100 day Mars transit mission. The MTBF growth factor required to achieve the same probability of failure with 1 fewer units is also indicated. These values assume that all repairs are completed successfully and there are no manufacturing defects, environmental effects, or unanticipated interactions.

$N$	MTBF/Endurance Ratio	MTBF Required for Mars Transit [hrs]	MTBF Growth Factor To Reduce $N$ by 1
1	999.5	26,386,800	N/A
2	22.0	580,800	45.43
3	5.2	137,280	4.23
4	2.3	60,720	2.26
5	1.4	36,960	1.64

Longer missions increase the probability that failures will occur, even for components with very low failure rates.<sup>7,8</sup> As a result, the MTBF required to achieve a high POS for a long-endurance mission grows quickly. Figure 1 shows the ratio of MTBF to mission endurance required to achieve a desired POS level for various levels of redundancy or spares, using equation 2. When only one unit is provided, the MTBF must be approximately 9.5 times greater than the mission endurance in order to achieve a POS of 0.9, which for critical systems corresponds to a P(LoC) of 1 in 10. For a POS of 0.99 or 0.999, the MTBF must be approximately 99.5 or 999.5, respectively. Put another way: to reduce the probability of failure on a 1,100 day Mars transit mission to less than 1 in 1000,<sup>a</sup> the MTBF for a single-string system would have to be greater than 3,000 years.

Critical systems for long-endurance missions such as these must take into account the fact that, for any reasonable MTBF value, failures will most likely occur. Therefore, systems should be designed to recover from failures, either by incorporating redundant elements or spare parts and a maintenance capability.<sup>7,8</sup> As shown in figure 1, the addition of redundancy or spares can significantly reduce the required ratio of MTBF to mission endurance. For the purposes of this paper, the term “spare” will be used to refer to any item beyond the initial unit, whether that item is incorporated directly into the system as a redundant unit or requires a maintenance action to replace the previous unit. From a reliability perspective, for a first-order analysis where repair time impacts (e.g system downtime, crew time requirements) are neglected, spares and redundancy are functionally nearly equivalent. Table 1 lists the ratios required for various values of  $n$ , as well as the corresponding MTBF (in hours) for a Mars transit mission. The addition of a single redundant unit reduces the MTBF requirement to just over 66 years. Each additional unit added reduces the MTBF requirement further; when five units are available (one initial unit plus 4 redundant units), the MTBF requirement is just over 4.2 years. Note, however, that these values are optimistic, and do not include other factors that could impact system reliability, such as manufacturing defects, environmental effects, unanticipated interactions.

Table 1 also indicates the impact of increased reliability the the number of units that must be carried to achieve the same level of risk. Starting from  $n = 5$  (an MTBF requirement of 36,960 hours), the MTBF must increase by a factor of 1.64. The next jump is a higher ratio; to reduce from 4 units to 3, the MTBF must increase by an additional factor of 2.26. This factor continues to increase exponentially as  $n$  decreases. In the context of maintenance logistics planning, this simple, single-item example shows that each additional spare saved by increasing reliability requires significantly more reliability growth than the previous one. The impact of reliability growth in more complex, multi-item scenarios is investigated in section IV, and this trend of diminishing returns is also seen in that situation.

The results of this single-item case illustrate the challenge of maintaining systems on long-endurance missions. Unreasonably high MTBFs would be required to provide a high probability of no failures occurring, so failures must be expected and accounted for with additional spares. To achieve a high probability of success, a mission must increase the MTBF of critical components, carry additional spares or other maintenance capability, or (most likely) some combination of the two. The amount of reliability increase required to decrease the number of spares required grows exponentially, and therefore in terms of logistics mass reduction produces diminishing returns. Decisions regarding reliability growth efforts must weigh the cost of increasing

<sup>a</sup>This baseline POS of 0.999 is selected to represent a notional target for maintenance logistics contribution to P(LoC) of  $10^{-3}$ ; note that, as discussed in subsection A, a mission that achieves this POS will have a P(LoC) greater than  $10^{-3}$ . This relationship between POS and P(LoC) is discussed in greater detail in other papers.<sup>13,14</sup>

reliability against the cost of carrying an additional spare, along with all other risks that are not captured by equation 2. Section III examines the time and financial costs associated with increasing reliability, and section IV examines the impacts in terms of in order to inform this trade.

### III. Costs of Reliability Growth

Several models of varying complexity exist to forecast the time and cost required to increase a system's reliability. The Department of Defense (DoD) Reliability Growth Management Handbook (MIL-HDBK-189C)<sup>6</sup> presents an overview of major models used for reliability growth planning and a discussion of key concepts. Most models focus primarily on the relationship between testing time and achieved reliability for a reliability growth program, which would then be used to inform program planning and cost assessments based on the cost of test time. Other models directly examine financial cost associated with reliability growth. Both time and financial cost considerations are discussed below.

#### A. Test Time

Most reliability growth models are based on the observation by Duane<sup>16</sup> in the early 1960s that, when plotted on a log-log graph for a variety of different systems, the cumulative average failure rate  $C(t)$  (defined as the number of failures  $N(t)$  observed up to time  $t$  divided by  $t$ ) forms a straight line with negative slope.<sup>16</sup> This slope,  $\alpha$ , is known as the reliability growth rate (or shape parameter), and an additional parameter  $\gamma$  is the scale parameter, or initial failure rate.<sup>b</sup> This result indicated that the cumulative failure rate at some future time could be forecast using a power law:<sup>6,16-18</sup>

$$C(t) = \gamma t^{-\alpha} \quad (3)$$

The instantaneous failure rate  $\rho(t)$  (i.e. the current failure rate at time  $t$ ) is the rate of change in  $N(t)$  per unit time:<sup>16-18</sup>

$$\rho(t) = \gamma(1 - \alpha)t^{-\alpha} \quad (4)$$

The reciprocal of equation 3 or 4 provides the cumulative or instantaneous MTBF, respectively. This learning curve model for reliability growth is known as the Duane Postulate.<sup>6,17</sup>

Other, more complex models have also been developed. For example, Crow<sup>19</sup> expanded upon the Duane model to implement it within a statistical framework, modeling failures as a Non-Homogeneous Poisson Process (NHPP) with a Weibull intensity function. The resulting model, the Army Materiel Systems Analysis Activity (AMSAA) Crow Planning Model (also known as the Crow AMSAA model or the AMSAA model) enables examination of reliability growth over multiple test phases as well as more advanced statistical analysis and monitoring of reliability growth processes.<sup>17,19</sup> Under this model, MTBF growth can be expressed based on the growth rate  $\alpha$  and an initial MTBF,  $MTBF_1$ , observed over some initial test period  $t_1$ :<sup>6</sup>

$$MTBF(t) = \begin{cases} MTBF_1 & 0 \leq t \leq t_1 \\ MTBF_1 \left(\frac{t}{t_1}\right)^\alpha (1 - \alpha)^{-1} & t > t_1 \end{cases} \quad (5)$$

The key parameter in modeling reliability growth is the growth rate  $\alpha$ . MIL-HDBK-189C<sup>6</sup> presents a table of historical estimates, noting that for time or distance based systems (as opposed to one-shot systems, like missiles) the growth rate estimates range from 0.23 to 0.53, with a mean of 0.34 and a median of 0.32.<sup>6</sup> Crow<sup>17</sup> also reports actual growth rates for various military systems, with an overall average growth rate of 0.40. However, when one-shot systems are removed, the average growth rate for the remaining 6 time-based systems is 0.36, a relatively close match to the estimates provided by MIL-HDBK-189C.<sup>17</sup> This growth factor – along with the maximum reliability increase that can be achieved (discussed below) – is dependent upon a wide variety of technical and management characteristics of a particular program, including:<sup>6,17</sup>

---

<sup>b</sup>Note that while Duane,<sup>16</sup> Crow,<sup>17</sup> and MIL-HDBK-189C<sup>6</sup> use the symbol  $\lambda$  to represent the scale parameter, this paper follows the convention of the 1981 MIL-HDBK-189<sup>18</sup> and uses  $\gamma$  in order to avoid confusion with generic failure rate  $\lambda$ .

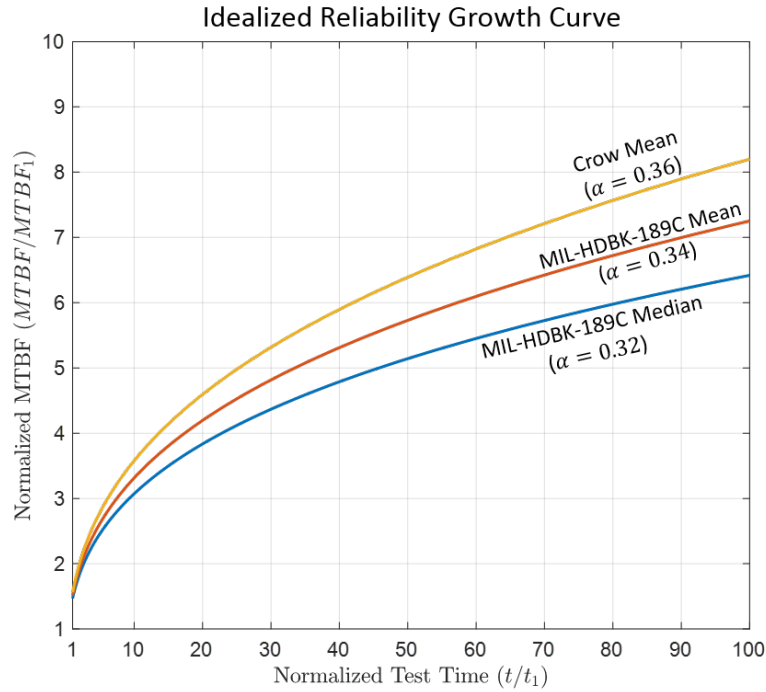


Figure 2. Idealized reliability growth curve, showing normalized MTBF as a function of normalized test time. Curves are shown for the three mean and median growth rates identified by MIL-HDBK-189C<sup>6</sup> and Crow.<sup>17</sup>

- the rate of failure mode discovery (which depends upon the failure rate of that particular mode),
- the time required to assess failure modes and implement corrective actions,
- the Management Strategy (MS), defined as the portion of the initial failure rate that will be addressed by corrective action if observed during testing, and
- the Fix Effectiveness Factor (FEF), which gives the amount of reduction in failure rate resulting from a corrective action for a particular failure mode.

Figure 2 shows the idealized reliability growth planning curve, using normalized time and MTBF, based on 5. Curves are shown for the three growth rates described above (MIL-HDBK-189C<sup>6</sup> mean and median and Crow<sup>17</sup> mean). Increased growth rate does result in a faster increase in MTBF, but in all cases the learning curve effect is apparent. Additional testing time to increase MTBF produces diminishing returns.

It is important to note that the reliability growth curves described by equation 5 and shown in figure 2 are idealized. Other factors strongly influence the maximum reliability that can be achieved and the rate at which it is achieved. For example, the last two factors that influence the growth rate, MS and FEF, also enable the calculation of the reliability growth potential  $MTBF_{GP}$ , or the theoretical upper limit to the MTBF that can be achieved<sup>6</sup>

$$MTBF_{GP} = \frac{MTBF_1}{1 - MS(\overline{FEF})} \quad (6)$$

where  $\overline{FEF}$  is the average FEF across all corrected failure modes. As equation 6 indicates, the higher the proportion of failure modes that are fixed (MS) and the higher the reduction in failure rate for that mode resulting from that fix (FEF), the higher the growth potential. Crow<sup>17</sup> and the DoD<sup>6</sup> note that MS is typically around 0.95, and MIL-HDBK-189C<sup>6</sup> also points out that it is “not prudent” to plan for an MS higher than 0.96 for developmental portions of systems.<sup>6,17</sup> MIL-HDBK-189C<sup>6</sup> also presents a table of historical FEFs; values range from 0.55 to 0.85, with a mean of 0.70 and median of 0.71.<sup>6</sup> Crow<sup>17</sup> recommends a FEF of 0.7.<sup>17</sup>

$MTBF_{GP}$  is a theoretical limit that is approached by systems as failure modes are identified and corrected; it is typically not achieved, and a margin of 0.6 to 0.8 is typically applied to  $MTBF_{GP}$  to obtain the goal MTBF,  $MTBF_G$ . Historically, the ratio of the initial MTBF to the MTBF of the matured system ranges from 0.15 to 0.47, with a mean of 0.30 and a median of 0.27.<sup>6</sup> Put another way, MTBF increases in reliability growth programs have ranged from a factor of approximately 6.7 to 2.1, and the median growth factor has been approximately 3.7.

It is important to bear in mind that additional test time alone does not improve reliability. Observation without alteration can enable a reduction of uncertainty around the reliability actually achieved by a system in its current state – which can be an extremely valuable process in itself, given the impact of MTBF uncertainty on maintenance logistics and risk<sup>20</sup> – but in order to change (and hopefully improve) the MTBF of a system, design or operational process alterations need to be implemented. Reliability growth is a process that requires the allocation of resources (both time and money) to perform tests, characterize failures and identify new failure modes, assess the system in order to determine how failure modes could be mitigated or have their rates reduced, and implement design or operational changes.<sup>6</sup> In this context, the slowing of reliability growth as test time increases makes sense: systems with high reliability fail less often, meaning that more test time is required to identify failure modes. In general, the reliability growth models assessed here indicate that the investment of time into reliability improvement produces diminishing returns (sublinear growth) in terms of increase in MTBF; put another way, the amount of testing time required grows superlinearly MTBFs are sought. Mathematically, for a growth rate  $\alpha$  between 0 and 1:

$$\text{MTBF Growth} \propto (\text{Test Time})^\alpha \quad (7)$$

$$\text{Test Time} \propto (\text{MTBF Growth})^{\frac{1}{\alpha}} \quad (8)$$

## B. Financial Cost

The financial cost of increasing reliability – including test time considerations described above as well as other costs, such as the cost of the redesign itself – has been described as having four key characteristics:<sup>21</sup>

1. The cost of low reliability components is very low.
2. The cost of high reliability components is very high.
3. Cost is a monotonically increasing function of reliability.
4. The derivative of cost with respect to reliability is a monotonically increasing function of reliability.

Mettas<sup>5</sup> proposed an exponential model for cost  $c$  as a function of reliability  $R$  that fits these requirements:<sup>5</sup>

$$c = e^{(1-f) \frac{R - R_{min}}{R_{max} - R}} \quad (9)$$

where  $f$  is the “feasibility” of increasing the component’s reliability (taking a value between 0 and 1, with lower values indicating that it is more difficult to increase reliability),  $R_{min}$  is the initial reliability (or minimum reliability, assuming reliability only improves), and  $R_{max}$  is the maximum achievable reliability.  $f$  and  $R_{max}$  depend upon the particular component for which reliability is to be improved, and the value of these parameters has a significant impact on the shape and value of the cost curve. However, in all cases the behavior is the same: cost grows exponentially with reliability. This cost model is not meant to directly capture financial costs, but instead to be used as a generic cost function for optimization and trade studies.<sup>5</sup>

Agte et al.<sup>7</sup> compared the model presented in equation 9 to results from a study conducted at the Charles Stark Draper Laboratory in 2009 to examine the relationship between MTBF and cost for lunar habitat avionics.<sup>c</sup> Their comparison found that equation 9 closely with the Draper results at various levels of complexity, including large units ( $f = 0.3$ ), medium units ( $f = 0.2$ ), and small units ( $f = 0.1$ ).<sup>7</sup>

While these models do not relate cost directly to MTBF growth as clearly as was done for testing time, they do indicate trends clearly. The cost of increasing the MTBF of large, complex items is lower than the

---

<sup>c</sup>The Draper study itself is an internal contract report,<sup>22</sup> and as of the writing of this paper the authors have not been able to access it directly. As a result, all descriptions presented here are based on descriptions by Agte et al.<sup>7</sup>



cost for simpler items; however, this relationship likely stems from the trend that simpler items are more reliable in the first place. Complex items may have “low hanging fruit” failure modes that can be identified and mitigated relatively easily. In general, cost grows exponentially with increased MTBF; mathematically:

$$\text{Cost} \propto e^{(\text{MTBF Growth})} \quad (10)$$

## IV. Reliability Impacts on Logistics and Risk

The illustrative example presented in figure 1 and table 1 examined the impact of increased reliability for a single-component system. This section examines the impact of variation in reliability on the maintenance logistics mass required for a DSH on a 1,100 day Mars transit mission.<sup>15</sup> Component MTBFs are varied to represent both an increase and a decrease in reliability for some or all of the DSH critical system repairable items. Variation in reliability is implemented by multiplying the nominal MTBFs by an MTBF multiplier,  $\eta$ ). Two analyses are performed in order to understand the impact of reliability impact on logistics mass and risk. First, the mass required to achieve a POS of 0.999 is calculated as a percentage of the mass in the baseline case (i.e. MTBFs at their current values) when  $\eta$  is varied between 0.5 and 10. Second, the POS achieved by the optimal manifest is examined when  $\eta$  is varied between 0.1 and 1 in order to examine the impact of reliability underperformance. In each analysis, three cases are examined in which  $\eta$  is applied to:

1. The top 10 components, in terms of contribution to corrective maintenance logistics mass
2. The top 25 components, in terms of contribution to corrective maintenance logistics mass
3. All components

For this analysis, only corrective maintenance logistics is considered – that is, spares carried in order to cover random failures. Spares required for scheduled replacement of life-limited items are not included.

### A. Maintenance Logistics Model Description

For this analysis, the demand for each individual type of spare is calculated using a Poisson distribution. It is assumed that all failures are independent, all repairs are completed successfully, and the impact of system downtime is negligible. The individual POS for each item is given by the CDF of the Poisson distribution (equation 2) as a function of that item’s failure rate and the number of spares provided. The overall POS is the product of these individual item POSs. A manifest optimizer is implemented to determine the combination of spare parts that achieves an overall POS greater than 0.999 for a minimum spares mass; this optimizer uses a branch-and-bound discrete optimization approach,<sup>11,23</sup> and accounts for scheduled maintenance by setting a lower bound on the number of spares that can be provided for a life-limited component. A more detailed description of this modeling approach is presented by Owens and de Weck.<sup>13</sup> A key difference in this application is that after the optimization is complete any spares that were allocated for scheduled maintenance are removed in order to isolate the maintenance logistics mass required for corrective maintenance.

Note that this analysis assumes that each item’s MTBF is deterministically known – that is, that there is no epistemic uncertainty. However, in application failure rate estimates still have a certain degree of uncertainty around them. This epistemic uncertainty can be captured in the form of a probability distribution, such as a lognormal distribution.<sup>24</sup> As new data become available via tests and operations, this distribution can be updated in a Bayesian process, such as the process implemented on the ISS.<sup>25,26</sup> However, significant amounts of test time and observations may be required, and the sample size of evidence gleaned from ISS experience and ground testing may not be sufficient to completely reduce this uncertainty, especially for complex systems such as the Environmental Control and Life Support (ECLS) system.<sup>27</sup> This uncertainty analysis is beyond the scope of this paper, but the impact of MTBF uncertainty on the relationship between mass and risk for deep space missions is discussed in detail by Stromgren et al.<sup>20</sup>

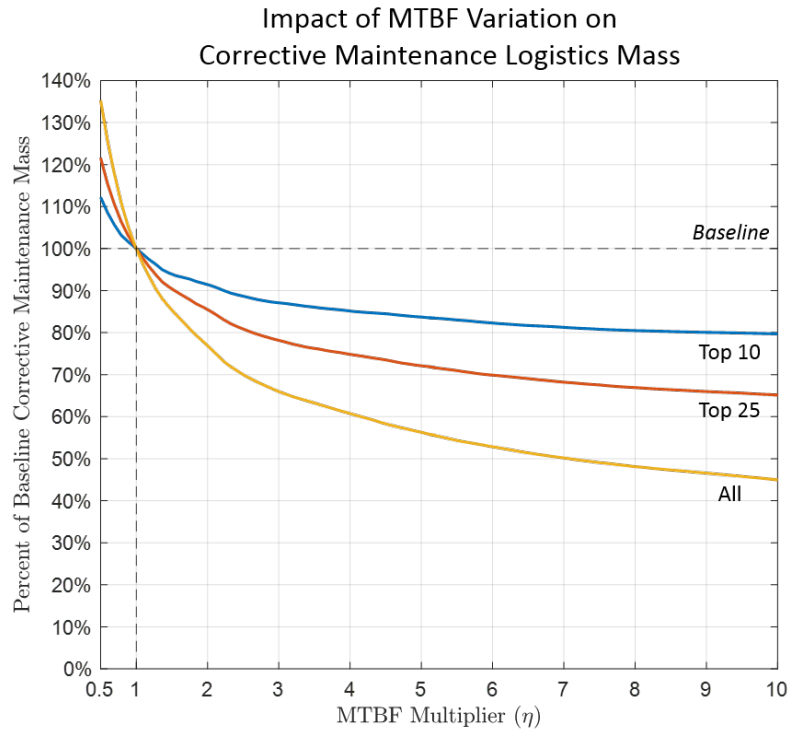


Figure 3. Impact of variations in MTBF on the mass required for corrective maintenance when the multiplier  $\eta$  is applied to the MTBF for all items (yellow) or the top 25 (red) or top 10 (blue) contributors to corrective maintenance mass.

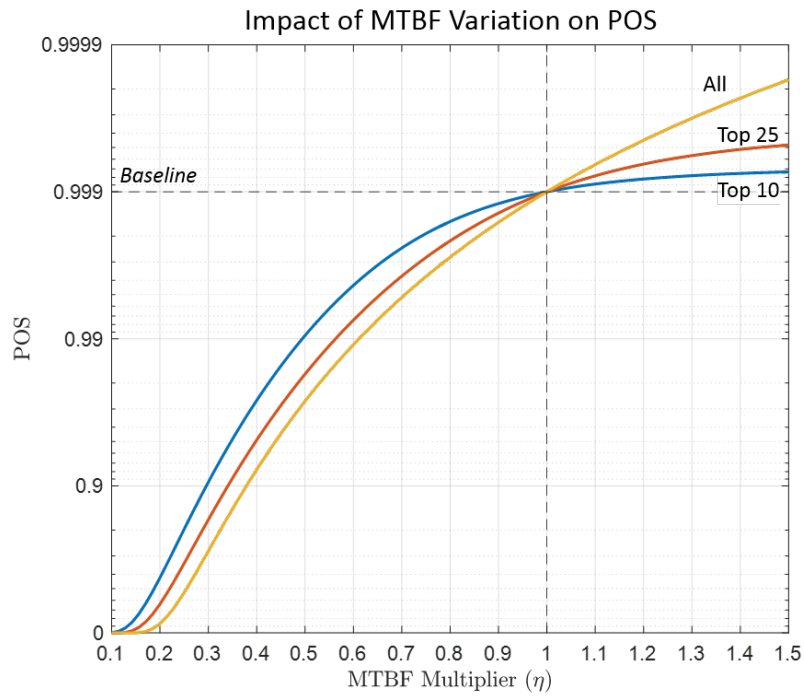


Figure 4. Impact of variations in MTBF on the POS achieved by the optimal manifest when the multiplier  $\eta$  is applied to the MTBF for all items (yellow) or the top 25 (red) or top 10 (blue) contributors to corrective maintenance mass. Note that the y-axis is plotted on a logarithmic scale.

## B. Results and Discussion

Figure 3 shows the impact of changes in MTBF on the spares mass required for corrective maintenance. In the baseline case ( $\eta = 1$ ), the mass of spares required for corrective maintenance is 10,089kg.<sup>d</sup> When the MTBF of all components is doubled, the corrective maintenance mass is reduced to approximately 76% of its initial value. Continued increase in MTBF reduces mass further, and when all MTBFs are ten times higher than their baseline values the corrective maintenance mass is just under 45% of its initial value. When only the top 25 contributors to corrective maintenance mass are altered, the mass percentages at  $\eta = 2$  and  $\eta = 10$  are 85% and 65%, respectively. When only the top 10 components experience increased MTBF, the corresponding values are 91% and 80%, respectively. Overall, increasing MTBF can decrease the mass required for corrective maintenance, but it produces diminishing returns. In addition, MTBF increase is most effective if it is applied to all components. When the number of components for which MTBF improves is reduced, the impact of improved reliability (in terms of logistics mass reduction) is also reduced.

Figure 3 also shows the impact of reduced MTBF. Corrective maintenance mass requirements grow much more quickly when MTBF decreases than they are reduced when MTBF increases, but again the magnitude of the impact is proportional to the number of components that experience a change in reliability. For example, the mass percentage when  $\eta = 0.5$  is applied to all components is 135%; that is, mass increased by 35%. To achieve a 35% decrease in corrective maintenance mass, MTBF must increase by more than a factor of three. For the top 25 and top 10 cases, the mass percentages at  $\eta = 0.5$  are 121% and 112%, respectively. These results illustrate the asymmetric nature of MTBF variation: decreased MTBF is more detrimental than increased MTBF is helpful.

Figure 4 explores this asymmetry further by examining the impact of  $\eta$  on the POS achieved by the optimal manifest from the baseline case. When MTBFs increase, POS also increases, though the amount of increase is limited by the number of components that experience higher MTBFs. Whereas a 50% increase in MTBF for all components raises the POS from 0.999 to 0.9998, if only the top 25 contributors to corrective maintenance mass are affected the resultant POS is 0.9995, and if only the top 10 items are affected the POS is just under 0.9993. Decreases in component reliability have a much more significant impact on system POS. An order of magnitude reduction in POS occurs when  $\eta$  is 0.61, 0.55, or 0.51, for the cases where all components, the top 25 components, and the top 10 components are affected, respectively. As  $\eta$  decreases, POS continues to decrease as well; the corresponding  $\eta$  values for a two order of magnitude reduction in POS are 0.38, 0.34, and 0.30, respectively. In addition, while reductions in POS are more significant when a greater number of components are affected, this effect is not as strong. Underperformance in reliability in even a small number of components can significantly impact the overall system POS. This makes sense, since system POS is the product of constituent item POSs, all of which are between 0 and 1; the lowest item-level POS sets an upper bound on the POS that can be achieved by the system.

It is important to note that figure 3 examines only the change in mass associated with corrective maintenance. This does not include mass for emplaced systems, consumables, or scheduled maintenance. These mass categories cannot be reduced by increasing MTBFs, since they are not dependent upon component reliabilities but rather more deterministic parameters such as the mass of components themselves, consumables consumption and recycling rates, and component life limits. As a result, the percent mass reductions indicated above do not correspond to total reductions in logistics mass, only reductions in one category of mass. The impact of MTBF on total mission mass requirements will be less than the results shown in figure 3.

In general, the benefits of increased MTBF (in terms of logistics mass saved from the baseline value) grow sublinearly; increased reliability produces diminishing returns. Mathematically, for an arbitrary mass savings growth rate  $\beta$  between 0 and 1 (unrelated to the reliability growth rate  $\alpha$ ):

$$\text{Logistics Mass Saved} \propto (\text{MTBF Growth})^\beta \quad (11)$$

The mass savings growth rate depends upon the number of units that experience MTBF improvements, as well as other factors such as the endurance of the mission, the POS requirement, and the particular set of equipment that is being spared for. This analysis showed that logistics mass savings grow fastest when all components experience reliability improvements, and the rate decreases as the fewer components are improved.

<sup>d</sup>Note that this value assumes that all MTBFs are deterministically known. When uncertainty is accounted for, this value will be higher. See Stromgren et al.<sup>20</sup> and Owens and de Weck<sup>14</sup> for an analysis of the impact of uncertainty.

## V. Discussion

### A. Assessment of Cost and Benefit Trends

The results presented above are not meant to represent an exact prediction of what the time, cost, and mass reduction potential of increased MTBF are, but rather an examination of how those values trend as effort is put into increasing reliability. These trends are captured in equations 8, 10, and 11, summarized below:

$$\text{Test Time} \propto (\text{MTBF Growth})^{\frac{1}{\alpha}} \quad (12)$$

$$\text{Cost} \propto e^{(\text{MTBF Growth})} \quad (13)$$

$$\text{Logistics Mass Saved} \propto (\text{MTBF Growth})^{\beta} \quad (14)$$

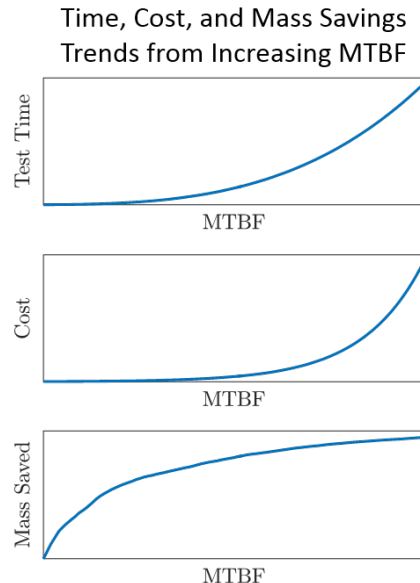
where  $\alpha$  and  $\beta$  are both constants between 0 and 1 that depend upon the characteristics of the system and mission at hand. These trends are presented graphically in figure 5. In general, time and cost grow as MTBF increases, with time growing superlinearly and cost growing exponentially. Meanwhile, the benefits of increased MTBF grow sublinearly; this agrees with the simple example shown in table 1, where the MTBF growth required to reduce the number of spares required increases with each additional reduction in spares.

These trends indicate that the cost (in terms of finances and test time required) of decreasing corrective maintenance logistics mass grows significantly and produces diminishing returns. In early stages, as “low-hanging fruit” are addressed and the easiest fixes to improve reliability are implemented, logistics mass requirements can be reduced for relatively low cost and test time. However, further efforts to increase MTBF will have less of an effect on system mass and will incur significantly more cost and test time. As noted in section II, future long-endurance missions would require unreasonably high MTBFs to provide a high probability that no failures will occur, and that therefore spares will have to be carried. The number of spares required can be reduced by increasing MTBFs, but high reliability will be expensive to attain, require a significant amount of test time, and have a diminishing effect on overall maintenance logistics mass requirements.

### B. Other Considerations

This analysis focused primarily on the benefits of reliability growth in terms of reduction in logistics mass requirements. However, there are other mission aspects that reliability might impact which should also be examined. For example, component MTBFs impact the number of failures that will occur during the mission; more reliable components fail less often, thus reducing demand for maintenance actions by the crew. This could reduce the crew time required for maintenance, as well as potentially reduce the risk of human error during maintenance (assuming that the probability of an incorrect maintenance action is not dependent upon the number of times the crew must execute that action, which may not be the case). This reduction in crew time required for maintenance would enable more crew time to be used for utilization, thus increasing the productivity and scientific value of missions. These considerations should also be weighed against the cost, test time, and mass reduction considerations discussed above.

The analysis presented in section IV examined only the spares mass required to cover anticipated failures. Each particular failure has aleatoric uncertainty surrounding it due to the inherently stochastic component failure process (characterized by the MTBF), and the corrective maintenance mass results presented in figure 3 represent the mass required to achieve the POS target when taking into account this aleatoric uncertainty. However, there may still be epistemic uncertainty present in terms of uncertainty in the MTBF values themselves. This uncertainty can significantly increase the amount of mass that must be carried to have a high confidence that sufficient spares are provided (see Stromgren et al.<sup>20</sup> for a more in-depth examination



**Figure 5.** Trends in test time requirements (top), cost (center), and maintenance logistics mass savings (bottom) as MTBF increases. These curves are for illustrative purposes only, based on the relationships defined in equations 12, 13, and 14, and do not represent exact results.

of this effect). As a result, when considering test time requirements for reliability growth, it is important to consider not only the test time required to identify and mitigate failure modes (i.e. improve reliability) but also the test time required to reduce uncertainty around the actual MTBF value. In addition, this analysis did not include common cause failures such as manufacturing defects, human error, or environmental effects. Operational experience on the ISS has shown that unanticipated issues continue to appear in human spaceflight,<sup>12</sup> even after years of testing and operations. These unanticipated issues will most likely continue to appear in future missions, especially when new environments are encountered for the first time. Common cause failures can significantly limit the risk coverage provided by spare parts and redundancy, since a common failure mode that causes an unexpectedly low reliability in a particular component is likely to also decrease the reliability of all of its spares.<sup>28</sup> This highlights the importance of testing in a relevant environment, since – as noted in section II – reliability characterizes a component’s ability to function for a given period of time within a given set of conditions.<sup>6</sup> If the actual operating conditions are different from the test conditions used to assess reliability, reliability estimates may be significantly different from actual values.

### C. Other Approaches To Maintenance Logistics Mass Reduction

Increasing reliability is not the only option to decrease maintenance logistics mass. This section gives a brief overview of other potential solutions that could be implemented.

#### 1. Direct Mass Reduction

The simple example examined in section II indicated that for long-endurance missions it is likely that several spares may need to be carried for each item in order to achieve high POS. While increasing MTBF may allow the number of required spares to be reduced, it may be more effective to invest resources into directly reducing the mass of each spare. The number of spares required for each item is then a multiplier on the total logistics mass saved. In addition, mass reduction is less expensive and time consuming to verify than increased MTBF since it is a deterministic value rather than a characteristic of a stochastic process.

#### 2. Lower-Level Repair

The analysis presented in section IV was based on an equipment list that consisted mainly of Orbital Replacement Units (ORUs), with some smaller components. ORUs are designed to simplify maintenance procedures in order to reduce crew time requirements for maintenance on the ISS. This is accomplished by packaging components and assemblies into easy-to-remove modules. However, this strategy for maintenance results in inefficient sparing, since good components are discarded when a failed ORU is replaced. A lower level of repair can enable more targeted maintenance that replaces only the component that has failed, thus reducing maintenance logistics mass requirements.<sup>13</sup>

#### 3. Parts Count Reduction and Commonality

One of the major drivers of maintenance logistics mass requirements is the fact that many different types of items need to be spared for, and that typically a single spare can only cover one type of failure mode. As a result, even though the expected number of spares that will actually be used is very small, there is no way to know *a priori* which particular spare will be required. For example, a logistics analysis by Cirillo et al.<sup>2</sup> estimated that, for the ISS, approximately 95% of the spares carried for corrective maintenance would not be used. This uncertainty means that a large number of spares need to be carried in order to achieve POS targets. A reduction in the number of different types of parts that have to be spared for – either by simplifying system design, incorporating commonality, or both – can help reduce logistics requirements by mitigating these impacts. Commonality in particular is a very valuable approach, since it enables a single type of spare to cover several different types of failures, rather than just one.<sup>2</sup>

#### 4. In-Space Manufacturing

The logistics challenges of future missions are unlike any that have been experienced in human spaceflight to date, and they may require entirely new approaches to maintenance logistics. ISM is a new technology that has the potential to significantly reduce maintenance logistics mass and mitigate risk on long-endurance

missions.<sup>14, 29</sup> ISM enables the creation of spare parts on demand from a common stock of raw materials, enabling flexibility in maintenance logistics that is not provided by a traditional spares approach. This capability enables the mass reduction benefits of commonality without forcing different components to have common design (which might otherwise have a detrimental impact on system performance). The flexibility provided by ISM also enables adaptable systems that can respond to unanticipated circumstances and mitigate the detrimental impacts of epistemic uncertainty in MTBF values. In addition, ISM enables the use of recycled or in-situ materials, opening the possibility of “closed-loop” maintenance logistics. Application of loop closure and In-Situ Resource Utilization (ISRU) have significantly reduced the logistics requirements associated with other spacecraft systems such as ECLS and propulsion, and an extension of this capability to maintenance logistics could also result in significant mass reduction. A more in-depth analysis and discussion of ISM applications and impacts is presented by Owens and de Weck.<sup>14</sup>

## 5. All of the Above (and More)

There is likely no single solution to the maintenance logistics challenges of long-endurance spaceflight. Instead, system development should examine combinations of possible solutions, balancing the costs and benefits of each against each other in order to reduce logistics mass and mitigate risk without incurring excessive development costs or test time requirements. The Lower Bounding Principle of Optimization states that when the design space is expanded, new solutions will be found that are at least as good, if not better, than solutions from the more constrained case.<sup>30</sup> Therefore, trade studies and optimization that remove as many artificial constraints as possible are likely to generate better solutions than design processes that fix or eliminate some options *a priori*. In the context of the maintenance logistics challenges examined here, these artificial constraints on the design space may be a fixed level of repair, fixed MTBFs, the assumption of no manufacturing capability, or inflexible part counts and commonality definitions. For example, Agte<sup>8</sup> and Agte et al.<sup>7</sup> showed that when both physical design variables and component failure rates are allowed to vary during optimization of long-endurance aircraft, better solutions can be generated than the case where either design variables or failure rates are varied while the other is fixed.<sup>7, 8</sup> Designers of future long-endurance crewed spacecraft should take advantage of all options available to them, examining the impact of each individual strategy as well as combinations of different approaches, in order to reduce maintenance logistics requirements and risk.

## VI. Conclusion

This paper examined the costs and benefits associated with increasing MTBF for long-endurance human spaceflight missions. Trends in test time, cost and logistics mass reduction resulting from increased MTBF were assessed via a review of reliability growth models found in the literature and an analysis of corrective maintenance logistics requirements for DSH critical systems on a Mars transit mission. In general, test time grows superlinearly, cost grows exponentially, and mass savings grow sublinearly as efforts are made to increase MTBF. Therefore, it seems unlikely that investment in reliability growth alone is a cost-effective approach to reducing maintenance logistics requirements and mitigating risk for long-endurance missions. Other potential strategies for logistics mass reduction were also discussed, including direct reduction of component mass, lower-level repair, simplification and commonality, and ISM.

These results are not meant to imply that reliability growth should not be invested in at all. Increased reliability is beneficial, and if it can be achieved at a reasonable cost and within a reasonable timeframe it should be attempted. However, system development and mission planning should carefully weigh the increasing costs of reliability growth against the diminishing returns that it provides. Reliability growth is only one option of many to reduce mass. The potential costs and benefits of all logistics reduction strategies – as well as any others that can be developed – should be examined, both as individual approaches to mass reduction and in combinations, in order to determine the most effective approach for future missions.

## Acknowledgments

This research was supported by a NASA Space Technology Research Fellowship (NNX14AM42H) and a technical consulting contract from Jacobs Engineering in support of the NASA HEOMD AES In-Space Manufacturing Project. The authors would like to thank Bill Cirillo, Kandyce Goodliff, and Chel Stromgren

for EMC DSH critical systems maintainability data and for their thoughts and input on this work. The authors would also like to thank Molly Anderson for her thoughts and input on this work.

## References

- <sup>1</sup>Jones, H. W., Hodgson, E. W., and Kliss, M. H., "Life Support for Deep Space and Mars," *44th International Conference on Environmental Systems*, No. ICES-2014-074, Tucson, AZ, 2014, pp. 1–15.
- <sup>2</sup>Cirillo, W., Aaseng, G., Goodliff, K., Stromgren, C., and Maxwell, A., "Supportability for Beyond Low Earth Orbit Missions," *AIAA SPACE 2011 Conference & Exposition*, No. AIAA-2011-7231, American Institute of Aeronautics and Astronautics, Reston, Virginia, sep 2011, pp. 1–12.
- <sup>3</sup>Hurlbert, K., Bagdigian, B., Carroll, C., Jeevarajan, A., Kliss, M., and Singh, B., "Technology Area 06: Human Health, Life Support, and Habitation Systems," Tech. rep., National Aeronautics and Space Administration, 2012.
- <sup>4</sup>Kennedy, K., Alexander, L., Landis, R., Linne, D., Mclemore, C., and Santiago-Maldonado, E., "Technology Area 07: Human Exploration Destination Systems Roadmap," Tech. rep., National Aeronautics and Space Administration, 2010.
- <sup>5</sup>Mettas, A., "Reliability allocation and optimization for complex systems," *Annual Reliability and Maintainability Symposium. 2000 Proceedings. International Symposium on Product Quality and Integrity (Cat. No.00CH37055)*, IEEE, Los Angeles, CA, 2000, pp. 216–221.
- <sup>6</sup>Department of Defense, "Reliability Growth Management Handbook (MIL-HDBK-189C)," 2011.
- <sup>7</sup>Agte, J., Borer, N., and de Weck, O., "Design of Long-Endurance Systems With Inherent Robustness to Partial Failures During Operations," *Journal of Mechanical Design*, Vol. 134, No. 10, 2012, pp. 100903.
- <sup>8</sup>Agte, J. S., *Multistate Analysis and Design : Case Studies in Aerospace Design and Long Endurance Systems* by, Phd dissertation, Massachusetts Institute of Technology, 2011.
- <sup>9</sup>Ebeling, C. E., *An Introduction to Reliability and Maintainability Engineering*, Tata McGraw-Hill Publishing Co. Ltd., New Delhi, tata mcgra ed., 2000.
- <sup>10</sup>Bertsekas, D. P. and Tsitsiklis, J. N., *Introduction to Probability*, Athena Scientific, Belmont, MA, 2nd ed., 2008.
- <sup>11</sup>Sherbrooke, C. C., *Optimal Inventory Modeling of Systems: Multi-Echelon Techniques*, Vol. 72 of *International Series in Operations Research & Management Science*, Kluwer Academic Publishers, Boston, MA, second ed. ed., 2004.
- <sup>12</sup>Do, S., *Towards Earth Independence – Tradespace Exploration of Long-Duration Crewed Space System Architectures*, Doctoral thesis, Massachusetts Institute of Technology, 2016.
- <sup>13</sup>Owens, A. C. and de Weck, O. L., "Increasing the Fidelity of Maintenance Logistics Representation in Breakeven Plots," *46th International Conference on Environmental Systems*, No. ICES-2016-344, International Conference on Environmental Systems, Vienna, Austria, 2016.
- <sup>14</sup>Owens, A. C. and de Weck, O. L., "Systems Analysis of In-Space Manufacturing Applications for the International Space Station and the Evolvable Mars Campaign," *AIAA SPACE 2016 Conference & Exposition*, No. (Submitted for publication), American Institute of Aeronautics and Astronautics, Long Beach, CA, 2016.
- <sup>15</sup>Simon, M. A., Wald, S. I., Howe, A. S., and Toups, L., "Evolvable Mars Campaign Long Duration Habitation Strategies: Architectural Approaches to Enable Human Exploration Missions," *AIAA SPACE 2015 Conference and Exposition*, No. AIAA 2015-4514, American Institute of Aeronautics and Astronautics, Pasadena, CA, aug 2015.
- <sup>16</sup>Duane, J. T., "Learning Curve Approach to Reliability Monitoring," *IEEE Transactions on Aerospace*, Vol. 2, No. 2, 1964, pp. 563–566.
- <sup>17</sup>Crow, L. H., "Planning a reliability growth program utilizing historical data," *2011 Proceedings - Annual Reliability and Maintainability Symposium*, IEEE, Lake Buena Vista, FL, jan 2011, pp. 1–6.
- <sup>18</sup>Department of Defense, "Military Handbook: Reliability Growth Management (MIL-HDBK-189)," 1981.
- <sup>19</sup>Crow, L. H., "Reliability Analysis for Complex, Repairable Systems (Technical Report No. 138)," 1975.
- <sup>20</sup>Stromgren, C., Goodliff, K., Cirillo, W., and Owens, A., "The Threat of Uncertainty – Why Using Traditional Approaches for Evaluating Spacecraft Reliability Are Insufficient for Future Human Mars Missions," *AIAA SPACE 2016 Conference & Exposition*, No. (Submitted for publication), American Institute of Aeronautics and Astronautics, Long Beach, CA, 2016.
- <sup>21</sup>Aggarwal, K. and Gupta, J., "On Minimizing the Cost of Reliable Systems," *IEEE Transactions on Reliability*, Vol. R-24, No. 3, aug 1975, pp. 205–205.
- <sup>22</sup>West, J., Claypool, I., Borer, N., and Odegard, R., "LSS Lunar Habitat Avionics Modeling Study – Task 3 Final Report, Reliability and Performance Implications of the Use of Commercial Grade Components (NASA/JSC Contract No. NNJ06HC37C)," 2009.
- <sup>23</sup>Hillier, F. S. and Lieberman, G. J., *Introduction to Operations Research*, McGraw-Hill Higher Education, New York, 7th ed., 2001.
- <sup>24</sup>Stamatelatos, M. and Dezfuli, H., "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners," 2011.
- <sup>25</sup>Vitali, R. and Lutomski, M. G., "Derivation of Failure Rates and Probability of Failures for the International Space Station Probabilistic Risk Assessment study," *Probabilistic Safety Assessment and Management*, Springer London, London, 2004, pp. 1194–1199.
- <sup>26</sup>Dezfuli, H., Kelly, D., Smith, C., Vedros, K., and Galyean, W., "Bayesian Inference for NASA Probabilistic Risk and Reliability Analysis (NASA/SP-2009-569)," 2009.
- <sup>27</sup>Bagdigian, R. M., Dake, J., Gentry, G., and Gault, M., "International Space Station Environmental Control and Life Support System Mass and Crewtime Utilization In Comparison to a Long Duration Human Space Exploration Mission," *45th*

*International Conference on Environmental Systems*, No. ICES-2015-094, International Conference on Environmental Systems, Bellevue, WA, 2015.

<sup>28</sup>Jones, H. W., “Common Cause Failures and Ultra Reliability,” *42nd International Conference on Environmental Systems*, No. AIAA-2012-3602, American Institute of Aeronautics and Astronautics, San Diego, CA, 2012.

<sup>29</sup>Owens, A., Do, S., Kurtz, A., and de Weck, O., “Benefits of Additive Manufacturing for Human Exploration of Mars,” *45th International Conference on Environmental Systems*, No. ICES-2015-287, International Conference on Environmental Systems, Bellevue, WA, 2015.

<sup>30</sup>Barton, P. I., “Mixed-Integer and Nonconvex Optimization,” 2011.