NASA/ TM-2015-218580

Low-Earth Orbit Reliability and Maintainability Paradigms and Their Application to Deep Space Exploration

Mariel Rico
The George Washington University
Washington, DC 20057

Melissa Flores
NASA Lyndon B. Johnson Space Center
Houston, TX 77058

National Aeronautics and
Space Administration

Johnson Space Center
Houston, Texas 77058

June 2015

NASA STI Program ... in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NASA Aeronautics and Space Database and its public interface, the NASA Technical Report Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at 443-757-5803

- Phone the NASA STI Help Desk at 443-757-5802

- Write to:
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/ TM-2015-218580

Low-Earth Orbit Reliability and Maintainability Paradigms and Their Application to Deep Space Exploration

Mariel Rico
The George Washington University
Washington, DC 20057

Melissa Flores
NASA Lyndon B. Johnson Space Center
Houston, TX 77058

National Aeronautics and
Space Administration

Johnson Space Center
Houston, Texas 77058

June 2015

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Available in electric form at http://ston.jsc.nasa.gov/collections/TRS

Nomenclature

CD	= Component Demonstrator
CONTOUR	= Comet Nucleus TOUR
DS	= Deep Space
DSE	= Deep-Space Exploration
DSH	= Deep-Space Habitat
EVA	= Extra-Vehicular Activity
ISS	= International Space Station
IVA	= Intravehicular Activity
LEO	= Low-Earth Orbit
MMSEV	= Multi-Mission Space Exploration Vehicle
MMOD	= Micrometeoroids and Orbital Debris
ORU	= Orbital Replacement Unit
PRA	= Probability Risk Analysis
RCS	= Reaction Control Sled
RMS	= Reliability, Maintainability, and Supportability
SOHO	= Solar Heliospheric Observatory
SRM	= Solid Rocket Motor
STS	= Shuttle Transportation System

As NASA develops more interest within Deep-Space Exploration (DSE), there are a variety of Reliability, Maintainability, and Supportability (RMS) concerns that need to be addressed to lower the risks of loss of crew or loss of mission. Low-Earth Orbit (LEO) RMS paradigms are no longer valid because of the nature of a Deep-Space (DS) mission. An overview research effort has been put forward to identify RMS practices from past human spaceflight programs, and then re-evaluate and apply them into DSE craft design and processes. Design considerations investigated include general hardware considerations, and the human factors affects on a DS spacecraft. This information will help spacecraft designers prioritize subsystems for maintenance therefore decreasing the likelihood of failures.

I. Introduction

As NASA further develops its plans for DSE, LEO practices cannot completely be implemented without raising the risk of a lost mission or crew. Although LEO paradigms for RMS cannot be directly applied to DS human exploration, methodologies from Shuttle Transportation System (STS), International Space Station (ISS), Constellation and other space-related missions can be modified so that they apply to DSE craft design, processes, and operations.

In the past, maintainability was not as much of a concern because missions were closer to Earth. Temporary fixes, even if they could potentially introduce long-term problems, were possible because missions were shorter. Resupply missions were possible because of the closer distance; therefore, missing a spare was not as dire. However, temporary fixes during a short-term mission eventually needed to be managed with a more permanent solution. In DSE missions, the opportunity for resupply missions may not be readily available. It is important to implement more efficient RMS standards to overcome these obstacles.

II. Definitions

To fully understand the role of RMS, it is important to fully understand what each term means in respect to designing, building, and operating a DS spacecraft.

Reliability refers to how well the system performs for a certain period of time (or number of cycles) under specific operating conditions. It also specifies what maintenance actions are necessary, the ease of maintenance, and the skill level in which the maintenance is performed. Reliability should be a primary focus during design and architecture development because it offers the first and most significant opportunity for positive influence within the system in terms of reliability. Low-reliability hardware or failures can easily jeopardize crew and mission objectives. It is best to research past space missions to determine how a component or subsystem might fail. Past missions account for how components or subsystems actually fail in space operation, rather than how they are expected to fail. This is especially true if the components are a part of a heritage mechanism.

Supportability, like reliability, is an inherent quality of the system, and should be developed alongside the design and manufacturing process. Supportability is the time and cost of logistics required to facilitate maintenance. Supportability factors that should be addressed in the elements of DSE include system documentation/technical data, supply support (including spares), corrosion prevention and mitigation planning, test and support equipment (such as embedding systems tests and diagnostics), packaging, handling, storage and transportation.

Maintainability is determined by the reliability and supportability of the spacecraft and its subsystems. Maintainability refers to preventative and corrective upkeep of equipment to return it to usable condition. Preventative maintenance includes inspecting, hard time removing, cleaning, servicing, and calibrating. Corrective maintenance refers to returning the equipment to useable condition. Scheduled and unscheduled maintenance refers to when the maintenance is taking place, and does not necessarily correlate with whether or not the maintenance is corrective or preventative. All maintenance will affect the efficiency of operations, which is undesirable and usually costly. Maintainability is dependent on available man-hours and materials, both of which are limited during DSE. The limit of man-hours will vary depending on the concept of operations. The vehicle will also need to remain maintainable when it is unmanned for any extended period of time.

These three concepts are important, and they all play a role in expanding the lifespan of the spacecraft. However, spacecrafts should still be expected to fail due to the nature of DSE. The past LEO paradigm that components can never fail is no longer valid. Components and subsystems will fail, but by implementing reliability and supportability into the design maintenance will be less demanding.

III. Deep Space Exploration Distance and Environmental Factors

LEO orbit has opportunities that are not available to DS missions because of the factors involved in DS. In order to make up for these losses, maintainability and supportability measures will need to be further developed.

One opportunity no longer available to the mission is the capability to resupply, refuel, and remove waste from the living quarters. DSE requires more transit time because the destination is further from the Earth. There is a long period of usage for the spacecraft and its subsystems, but fuel and supplies are limited to minimize mass for the entirety of the mission. Assemblies can no longer be delivered as needed, just as waste cannot be brought down to Earth by another space vehicle. Maintenance cannot wait for return to Earth, like many of the shuttle mission complications. There is also a limited amount of storage space for spares or any other equipment at the beginning of the mission. Any part of the spacecraft and any subsystem will need to be repairable and repaired by the crew or remotely with robotics with any supplies or tools that are readily available to them.

Being in space for a longer time period also elongates the exposure to natural space elements. Equipment will be subjected to low or no pressure, varying degrees of temperature and radiation. There are two concerning types of radiation to be aware of: solar flares and galactic cosmic radiation. LEO operations are within the thermosphere and the Van Allen belt, both of which protect past missions like STS and ISS. Even without the Earth's natural atmosphere protecting the vehicle and crew, the ISS has a shield that protects it from solar flares. A shield, although heavy, can be implemented in DSE. Cosmic radiation provides a stronger threat. Cosmic rays are less harmful but constant in the environment. There is no way to fully shield the crew and spacecraft from any damages without carrying a large shield that can significantly weigh down the transport vehicle. Even with the shield, radiation can still disrupt performance levels and leave permanent damage to exposed equipment.

Similar to cosmic rays, micrometeoroids and orbital debris (MMOD) are also a threat in deep-space exploration. There is about one-third the amount of MMOD in DS as there is in LEO, but the risk of being hit is dependent on exposure time and the surface area of the spacecraft and its shielding. The spacecraft could experience less or more risk depending on those factors. Larger spacecrafts are at a higher risk of being hit by MMOD. There is also a long-term exposure in DS, so the risk of MMOD is proportionally higher based on how long the spacecraft is in use. [1]

These are only a few of the problems engineers will have to face when designing and performing missions. Long-term solutions to these constant factors can be found by investing in RMS measures.

IV. Design Considerations

A. Management's Role

Short-term management decisions can have a long-term affect, so management plays a large role in the outcome of the product. At the management level, there is a "better, faster, cheaper" philosophy. This philosophy hurts the development of RMS systems, which in turn hurts future operations. Both unmanned and manned testing is required to fully develop RMS systems. Although testing is considered costly, not having enough or proper testing can be considered more hurtful to the mission in the long run. Proper testing has the capability to find subtle design weakness that can potentially lead to bigger problems during operations. Proper testing also gives experience to the technology, highlighting the reality of what the spacecraft is capable and incapable of.

Modeling and simulations are initially more cost-effective than testing, but modeling and simulations can be misleading. Relying on models and simulations instead of testing can lead to misleading maintenance concepts that only work on the computer. Hardware or software that cannot be maintained on Earth is not viable for operation in space. Any modeled or simulated solutions need to be tested to be confident that it is possible during operations. The development of RMS practices will save time during actual space operations, which in the long term will save money because there are less unexpected obstacles.

Maintenance will always conflict with the efficiency of the operations, which is costly in terms of expense and time. The more data collected from testing, the more reliable RMS designs can be. Maintenance in space will most likely take longer than expected, and it will be more difficult than maintenance on Earth. Investing in the development of RMS practices will save time during actual space operations. If potential hazards are accounted for in the beginning, the expenses throughout operations should be more reasonable.

B. Design Selection

Even with the assumption that everything onboard can be maintained and supported, maintenance can only be as reliable as the system itself, so the initial design must be reliable. To ensure that this philosophy is accounted for, it

[1] Christensen, Eric. E-mail Correspondence. Houston, TX. 18-19 July, 2012.

is best to design the system as if it is expected to work correctly for its first flight. It cannot be assumed that there will be maximum performance or minimum weight.

Design considerations need to be made to avoid premature failures. Stresses that need to be accounted for include stresses applied by surround parts and part changes and instantaneous stresses. How stress affects the components working together vary from part to part and from manufacturer to manufacturer. Instantaneous stress refers to the instantaneous changes on the part caused by the environment. Harmful environments can include temperature, vibration shock, and electrical stresses and transients. Environmental effects combined can cause a component to prematurely fail because the stress exceeds the component's tolerance levels.

There are two ways to reduce a part failure rate. One way to reduce stress levels so that the probability of exceeding the component strength is less. This is not always possible, so a second method is implemented. The alternative method is known as parts derating. Parts derating increase the parts strength for a higher factor of safety. An additional advantage to part derating is reducing internal operating temperatures and decreasing the chemical time-temperature reaction, which causes part aging and parameter drift.

Although heritage designs can initially save money, they can also be hazards to the system if not correctly integrated. It may be more cost-effective to consider new designs rather than modify a heritage design. When heritage designs are implemented, designs need to be re-evaluated to make sure they are properly integrated into a system. Despite past performances, systems in one application may or may not be appropriate for a different application.

Comet Nucleus Tour (CONTOUR) is a prime example of incorrectly implementing a heritage design. CONTOUR is a spacecraft designed to study the physical and chemical properties of two different comets during their visits to the inner solar system. During the system engineering design process, there was a flawed heritage assumption that the system would function correctly. The system was not reviewed properly, so there was a limited understanding of how the Solid Rocket Motor (SRM) plume heating functioned in space and the type of conditions needed for operations. The heritage SRM was then improperly installed into the spacecraft. During the mission, the spacecraft overheated which cased structural failure. The spacecraft split into several pieces, and the mission was lost. Heritage designs cannot be assumed to function properly unless they are properly tested and integrated. False assumptions can lead to a variety of consequences and even a loss of crew or the mission.

The failed CONTOUR mission also illustrates how important failure testing is. Failure testing indicates how things fail before any components are in operation. Using this knowledge, ground control and crew members can understand how and why things fail. This knowledge can be used to determine what kind of maintenance needs to be implemented in order to prevent further damage.

Another method of reliability in a system is redundancy. Redundancy can be advantageous to the maintainability of any spacecraft. Two possible types of redundancy that can be implemented into a spacecraft's design is internal and standby redundancy. Internal redundancy creates a higher level of failure tolerance, but it does allows the Orbital Replacement Unit (ORU) to fail without a replacement. A single failure should not cause a loss of a redundant path for internal instrumentation redundancy. Standby redundancy allows operations to continue uninterrupted after the failure of an ORU. It also allows crew members to defer maintenance to a more convenient time.

For compatibility with another spacecraft, including international spacecrafts, the units used for designs and hardware should be considered. For systems to be completely integrated, the components will need to be compatible in form, dimension, and function. Having identical units allow for better interfacing, and potentially supply more spares to either system.

Using a combination of metric and English units is possible, but it can lead to many complications. For example, there may be unnecessary duplications without creating redundancy within the system. Having a combination of units can also convolute the requirements in documentation because unit conversions may not be accurate and there are two sets of units. This was an obstacle on ISS, because there were tools that became specialized because they could not be implemented on other international modules.

C. General Design Considerations

The RMS support system should be developed alongside the design process of the spacecraft and its subsystems for efficiency. Although every spacecraft is different, there are general RMS guidelines that can improve RMS any design.

It is understood that in DSE components will eventually degrade, and fail. For a system to be more maintainable, it is important to determine what degree of maintainability is required. It may be more viable to leave a failed component within the system if the spacecraft is still operable because human error could make the situation worse. If a repair is required, it may be wiser to replace a part rather than an entire assembly. Having spare components

instead of spare assemblies contribute to a lighter payload. Making components on the spacecraft as standard as possible also increase the amount of spares available, allowing parts to replace each other without using spares. Two similar, yet non-interchangeable parts should not exist within a design because at least one of each type of unit will need to have its own spares. Following this protocol reduces the number of spares needed on-orbit.

It is important to note that sparing will also depend on preventative maintenance. Preventative maintenance is helpful because it can maximize human performance, but it requires strategic planning. Preventative maintenance offers an advantage to corrective maintenance because a failure has not occurred yet. It is easier to have a planned maintenance for a subsystem than it is to respond to an unplanned failure.

When writing procedures it is important to plan for preventative maintenance accordingly. Replacing or repairing a component before its full lifespan can be wasteful. The limited supplies of a DSE mission cannot afford to use spares without proper planning. Allowing the component to reach a critical state can force crew members to respond to a failure. The goal of preventative maintenance is to minimize or even eliminate the need for an unplanned maintenance. Preventative maintenance offers the opportunity to plan for failures, allowing crew members the opportunity to defer maintenance without impacting operations.

When an individual component fails, internal or stand-by redundancy within the spacecraft should keep operations running until the crew is able to schedule maintenance. This reduces the number of Extra-Vehicular Activity (EVA) excursions needed by maximizing the number of activities that happens during each EVA. Reducing the number of EVAs will prevent the crew from over-exhaustion, reduce costs, and reduce time preparing for each EVA. It is also safer for the crew if they can avoid EVAs.

It is important to verify what component is malfunctioning before an EVA because an EVA will require more time than expected. A labeled caddy that can make all of the needed tools and small parts easily accessible will help organize crew members and prevent real-time confusion or complications.

Tools used during a DS mission can also contribute to supportability. Tools used during the mission should not be specialized unless there is no other alternative. If the elimination of a tool does not excessively slow or exhaust the user, it should be eliminated. It is best to use general tools that anyone can find in a hardware store with slight modifications to respond to the zero-g environment. These modifications should also allow the tools to be used in EVAs and Intravehicular Activities (IVAs) if possible, because it lowers the number of tools needed onboard.

An example of the multiple uses within a single tool is STS-117. During launch, the thermal blanket insulation had pulled away from adjacent thermal tiles. The shuttle’s robotic arm and an extension boom-mounted sensor system were used to inspect the heat shield along the shuttle’s nose and wing edges. Seven days later, the blanket was repaired within two hours during a six-hour EVA with a medical stapler and pins. In this case, creative use of the medical stapler provided crew members another way to maintain the shuttle. It is not necessary to have two staplers, one for EVA and the other for IVA, when one can accomplish both tasks.

Redundancy can be advantageous to the maintainability of any spacecraft. Two possible types of redundancy that can be implemented into a spacecraft's design is internal and standby redundancy. Internal redundancy creates a higher level of failure tolerance, but the ORU can still fail without a replacement. A single failure should not cause a loss of a redundant path for internal instrumentation redundancy. Standby redundancy allows operations to continue uninterrupted after the failure of an ORU. It also allows crew members to defer maintenance until a more convenient time.

RMS designs also rely heavily on troubleshooting systems. False troubleshooting can seriously impact a mission. An example of this is the Solar Heliospheric Observatory (SOHO). SOHO was experiencing software glitches that caused the satellite to go into safe-holding. There were three gyros used to control the spacecraft. Gyro A was used for attitude control, B was used for detecting faults, and C (normally off) was used to control safety mode. Gyro A was turned off as intended, and B fixed itself. Soon after the maintenance, Gyro B’s reading diverged from what C expected, and the satellite entered safe mode after two hours. Instead of analyzing why the satellite entered safe mode, the crew assumed that B was misbehaving, and turned the gyro off. The satellite, lacking an active gyro, lost control and was not recovered until several months later. This mishap could have been avoided had accurate and thorough troubleshooting occurred, instead of making hazardous assumptions. Another design factor that could have been implemented to prevent this event is through providing telemetry to describe why the satellite entered safe mode in the first place.

The procedure for maintainability is detecting the hazard, identifying the fault, isolating the failure so that it does not affect the other subsystems, repairing the system for long term use, and verifying that the repairs are functioning properly. This procedure is crucial in DS to prevent failures from reoccurring.

D. Design Considerations to Maximize Human Performance

One of the greatest assets to space exploration is human engineering. The crew should be treated as a system component and be considered within the initial design concept. Considering crew operations after the initial design concept will require significant changes within designs, which are costly in both time and resources. The productivity of the crew determines the overall performance of the mission.

Since the success of the mission relies heavily on the crew, it is important to train them in an appropriate manner. In a DS mission, the crew will not necessarily have steady communication with ground support. The crew will need to be trained so that they do not have dependence on ground control. DSE also does not allow crew changes, so the crew onboard will need to be skilled in maintenance. Despite not having an alternative crew, this can be beneficial because the crew onboard will be well-versed in the operations of that spacecraft.

The crew must be provided with the means to support themselves in order to be effective. The resources available to the crew are limited to what was brought into space. The spacecraft needs to be designed in a way where all subsystems are accessible to the crew for maintenance. There should be no unit, ORU, or installation that needs to be removed in order to gain access to another unit. Maximum clearances and accessibility should be embedded into the designs to minimize potential damage. Adequate visibility and lighting are also a priority. If the subsystem is not accessible, then it is not maintainable. Equipment that is considered dangerous to personnel is also not maintainable. The outside of the spacecraft will need the proper restraints so that all is accessible during an EVA. Restraints should allow flexibility and versatility in the zero-g environment during IVAs or general operations within the spacecraft. Possible restraints include foot loops, velcro tape, handholds, suction cup shoes, sleeping restraints, waist/seat restraints, and lap belts. Systems need to be designed in a way that allows the crew to perform an IVA instead of an EVA. The crew must also be provided with all of the tools, like spare parts or equipment, to perform the repairs. These spare parts and equipment need to have enough damage resistances to ensure that there are no handling difficulties. The crew should also be trained with the same tools and equipment so that they are familiar with its usage, as it is difficult to do repairs without the tools practiced with. Designs need to account for momentum, inertial loads or ORUs, crew members, and robotics devices. Lastly, the crew must be trained so that they have the knowledge to carry out necessary tasks.

Without a continuous communication with ground support, training the crew becomes more critical than before. The currency of the crews' training can become outdated because DSE operate through an extended period of time. On-board training materials should be provided and updated as used so that resources are available to the crew. Procedures provided for training should be step-by-step, and shorted if possible to improve response time. These procedures should be developed from past space flights; it is the only data that can accurately predict what is possible for human performance in space. Maintenance action histories are especially significant. The nature of DSE, as well as any space exploration mission, will face unexpected complications throughout the mission. Although designing a training program for something unexpected is difficult, training the crew to identify normal and abnormal properties of the spacecraft can prevent real-time confusion.

The crew is responsible for documenting and collecting data from all maintenance procedures involved during operations. The systems can be electronically designed for recording where faults occurred, and what may have happened to ease this tedious process. Memory must be available for electronic records storage. Records should include what the problem was, when it happened, and why the abnormality occurred. All types of maintenance need to be accounted for. Recording malfunctions and maintenance help keep the crew fully aware of the state of the spacecraft. Having records also allows the crew to have an organized way to retrace actions if necessary. The data collected can also be applied to later missions as a resource for reliability standards and possible maintainability methods.

E. Limitations of Human Performance

The presence of a crew can create high reliability without excessively high reliability hardware. When integrated correctly, human factors reduce maintenance time and cost, and act as a backup during malfunctions. A STS probability risk analysis on the human reliability in response to failures reduced the risk of loss of crew or loss of vehicle by ninety-one percent.[2] Despite the versatility of skills that humans bring to a mission, they impose a lot of requirements and constraints on the equipment designs. Human engineering is dependent on the human's size, strength and capability to the do the tasks. The environment, like warmer temperatures versus colder temperatures, can reduce or increase human productivity. Every crewman will experience a different reaction to being in space,

[2] Hamlin, T., "Human Reliability Analysis Methodology and Modeling Results from Space Shuttle Program," NASA JSC Safety and Mission Assurance [PowerPoint slides], 28 February, 2012.

especially when exposed for extended periods of time. It will take time for crew members to adjust to the space environment.

Crew members also play other roles on the spacecraft such as observer, lab technician, and experimenter. They cannot be expected to only maintain the spacecraft and its subsystems during the operations because they have other responsibilities. Multiple operations will cause exhaustion, which can contribute to an increase of human errors. Equipment needs to have safety precautions to safeguard against a maintenance crew member's lapse of attention. DSE missions are long-term, closed ecological systems, so all crew members, hardware, and subsystems interact and affect each other. One subsystem malfunctioning will affect everything else in-turn.

Even without any subsystems malfunctioning, the overall noise levels within living quarters can affect the crew. The living quarters of a DS vehicle will be compact, and the crew will be expected to endure long periods of time within the spacecraft. Noise can be produced by various components within the system, such as fans, motors, pumps, valves, regulators, oscillators, thruster firings, or other equipment. These noises will be simultaneous to each other, and continuous. Limiting noise will help conserve the crew's hearing, improve the habitability of the quarters (affecting the crew's sleep, fatigue, or comfort levels), and ease communication between crew members and with ground. There are two ways to reduce noise levels. One is to minimize the noise level at the source. This can be done by interrupting or absorbing vibrations before they become airborne. The second way to preserve hearing is to provide each crew member with personal hearing protection. Currently, crew members operating within the ISS have implemented this technique.

Since humans are considered to be a subsystem within a spacecraft, human errors can negatively impact operations. One example of human error occurred during an EVA on STS-126. During the EVA, one of the grease guns released Braycote grease into the tool bag. While the astronaut was trying to clean the tool bag, the bag started to drift away from her. When the astronaut realized that the tool bag had become lose from its tether, it was too late to reach for it. Objectives for the EVA were still completed by sharing the tool bag of another crew member. The tool bag and contents had an estimated cost of $100,000.

The loss of the tool bag became a limiting resource during the EVA, and is a loss of costly items. Since the mission was in LEO, the tools could eventually be replaced. There may not be an opportunity to replenish lost supplies in DS. The tools available are limited to what the crew brought into space, so the loss of anything can lead to major complications. Assuring that tool bags and other tools are properly tethered can prevent the loss of supplies during EVAs.

There are other preventative measures to further ensure the safety of the mission and the crew, even when a human error occurs. It may be more sensible to use automation, robotics, or a combined effort between the two. Using automation and robotics are less exhausting, less time consuming, and less costly than performing an EVA. It also allows for a faster time response, so it improves reliability without deferring maintenance. Safety is improved because locating the ORU is done within a pressurized area instead of an external space location. Automation and robotics can also enhance human decisions for on-site troubleshooting and repair capabilities. Automation and robotics need to be maintained, but their capabilities ultimately enhance maintainability.

An additional method to reducing human error is to eliminate the possibility of certain types of errors from even occurring. When a malfunction occurs, it is important to properly identify what happened, where it is located, and how to repair the damage before the actual maintenance. Falsely identifying and repairing any units could lead to unnecessary tampering with the systems raising the potential for mishaps.

Hardware can be designed to impose correct measures upon the crew to avoid induced damage. During any mission, many connectors will be implemented throughout the spacecraft, but simply connecting them incorrectly can cause major problems. The design and the location of each connector should be in place before any connection cross between lines or cables. All connectors should have the capability to be blindly mated, and should be designed in a way that does not allow improper attachment or alignment. Any connector involved in EVA should also be EVA replaceable.

Fasteners, like connectors, are also widespread throughout the entire spacecraft; therefore, their designs should also be fail-safe. Similar to connectors involved in EVAs, fasteners involved in EVA should also be EVA replaceable. The variety of fasteners, in size and type, should be minimized to reduce sparing. Fasteners should also be quick-release, self-aligning, easy starting, low torque or force operating, require a minimum amount of strokes or turns, and should not require tools.

Another way to have hardware impose correct measures is to have self-calibration, self-adjustment, and self-testing within each ORU. These procedures should run after any ORU is installed or replaced. Calibration or adjustment tools that need a crew member for operation can easily be misread or inaccurately operated. There is also a possibility that ORU replacements may not even need adjustments or calibration if there is adequate allowance or matching interface tolerances.

F. Maintenance When Unmanned

There may be periods of time when a crew is no longer living within a spacecraft. During this time, the spacecraft needs to be maintained so when the crew returns, the spacecraft will be habitable. Maintenance is backlogged when the spacecraft is unmanned. Maintenance procedures for satellite missions can be implemented because those spacecrafts are not necessarily serviced by a crew.

Satellites rely on a safety mode when they are waiting for ground to intervene. These safety modes are simple, robust, and available during all phases of the mission. During safety mode only critical subsystems operate. Operations are kept to minimal but sufficient levels. Safety mode should be kept independent from hardware and software in normal mode to ensure isolation within the system. Subsystems that are not directly related to the survival of the spacecraft are turned off to conserve energy. Critical systems operating include positioning and location controls, temperature controls (to keep the spacecraft from becoming too hot or too cold), and the troubleshooting system. When there is a software or hardware mishap, the safety mode isolates the fault and reconfigures itself to continue minimum activity. These satellite RMS paradigms can be implemented to an unmanned spacecraft during DSE because of the lack of crew.

Another way to maintain a vehicle when a crew is not available is through the use of robotics and autonomous systems. Telerobotics is especially helpful because the robot will be operated by a human on ground in real-time. Instead of backlogging maintenance until the crew's arrival, the crew can work on the robot from Earth. Telerobotics can also be used for a faster response time.

Robotics designs will need to be compatible with the spacecraft. It should be recognized that robotics should not be relied on for precise positioning and force or torque control. There may be input movements that the operator cannot completely control. Robotics may also experience vibrations making it difficult to control. Design considerations include trajectories, access, alignment, grappling points, the number of operations or motions required for the precision of motion or force controls, the elimination of complex interfaces, and ORU identification.

Despite the advantages that robotics and automation systems can bring to the maintainability of a spacecraft, these systems will also require maintenance and will need to be designed accordingly.

V. Current and Future Efforts

A. Efforts within DSH to Improve RMS

There are current efforts to implement RMS lessons learned from LEO missions to DSE efforts. Deep-Space Habitat (DSH) is a multi-center NASA effort to create a more permanent habitat in deep-space to enable human exploration for multiple destinations.

Currently DSH is in the Concept Demonstrator (CD) phase. It is scheduled to go through a mission operations test in Fall 2012. This test is going to be used to evaluate technologies and human factors through mission simulations in a Habitation Development Unit. This will test the crew during simulated DS nominal activities, as well as an unplanned maintenance scenario in response to damage from MMOD. The crew will be unaware of this scenario. The MMOD damage will supposedly penetrate the hull and damage an external avionics box. The crew will then be expected to replace the avionics box (although only a portion of the real activity will occur). An IVA will also take place to repair the hull damages. The testing will also address a simulation refresher training for system check out and undocking the return vehicle for the return to Earth. This is a valuable test because it can predict how the crew will perform a check-out process after a refresher training course.

The next generation CD will be built up within a 20' vacuum chamber that provides a sealed facility for data collection, accurate input/ output identification, controlled thermal and efficiency levels, and other controlled environments. Information from these tests will be used to determine if the DSH is ready for a controlled but lower pressurized environment. The DSH CD will also be used to identify the level of redundancy required for the vehicle, develop a mission operations/crew autonomy concept, increase systems reliability and buy down developmental risks.

The DSH CD will be designed to facilitate maintenance and repairs for itself, and the other spacecrafts that are dependent on it. RMS systems include the capability for telerobotic control of remote assets to perform maintenance on electronic, mechanical, and soft goods. The DSH CD maintenance and repair facilities are also designed to provide the proper restraints, fixtures, and horizontal workspace for components removed from assemblies that need to be serviced.

The DSH CD will also be capable of the following maintenance capabilities: soldering, sheet metal bending, drilling, metal cutting, metallurgical analysis, bonding different surfaces (such as metal and composites), electronic analysis, computer inspection/ testing, computer-aid design modeling, material handling, precision hand tool manipulation, soft goods sewing, cutting, patching, and suit leak testing. 3-D printing is also available in the CD, but

there is still testing to deal with off-gassing, smell, and other things that may negatively impact the crew. All of these maintenance capabilities will assist the future crew of DSH and its other vehicle counterparts with sparing, and repairs which are vital to the success of the mission.[3]

B. Efforts within MMSEV to Improve RMS

Multi-Mission Space Exploration Vehicle (MMSEV) is an EVA and robotics vehicle system designed to optimize human performance.

Engineers recognize that although it is natural for maintenance procedures to be developed after building the vehicle and it subsystem, it is not necessarily the best approach. The mass and volume of a spacecraft will be limited because of the nature of DSE. Accounting for reliability and supportability early in the design process will help limit the mass and volume of the spacecraft, and provide clearer and more consistent guidelines. Having guidelines presents the opportunity for spacecrafts to be more closely integrated with each other regardless of each vehicle's architecture, mission, or destination. In regards to MMSEV, there are currently efforts to integrate the project with DSH. This allows MMSEV to have the opportunity to refuel, as well as share tools and resources, provided that there is compatibility between the two systems. A list of common tools is currently being compiled and evaluated to see where there is redundancy.

MMSEV recognizes that the duration of the mission will determine what tools need to be available to crew members. MMSEV is also trying to determine if the cost of having one set of tools for IVA and EVA is feasible, which can improve efficiency significantly. There is also an effort within MMSEV to standardize the variety of fasteners being used. Sockets and bit holders within the fasteners are being designed to be adaptable with a standard 3/8"square. Standardization gives access to three other readily available tools and eliminates one specialty tool. The number of fasteners is also being reduced, which lowers the number of sockets and bits needed.[4]

C. Recommended Safety Analysis for Future Missions

Once designs are more mature (but still in its early stages), the next step is to implement risk analyses. Performing Probability Risk Assessments (PRA) can be advantageous to the design of spacecrafts. PRA uses reliability data from other spacecraft or similar hardware to determine redundancy, sparing, and other important RMS factors within a spacecraft design. Fault Tree Analysis can also be beneficial for engineers because it can be used to identify hazards and critical hardware components. Once critical hardware is determined, one could perform a Failure Modes and Effects Analysis to further analyze the component.

Conclusion

Direct application of LEO RMS paradigms to DSE is not a viable option because of the nature of DSE. Environmental difference, the extended length of the mission operations, and the limited contact with Earth are some of the factors that need to be considered throughout the design and mission operation. The spacecraft will need to be designed and operated to maximize RMS practices to properly adapt to DS. The modification of LEO RMS paradigms provides an invaluable amount of knowledge to maximize efficiency throughout the mission. Concentrating on RMS early within a spacecraft design ensures the safety of mission, leading to a more successful mission.

Acknowledgements

M.R. Author would like to thank Melissa Flores for the opportunity to intern with her. Her guidance throughout the research effort was invaluable. Dawn Thomas, Hector Chavez, Maria Pulsonetti, and Vuong Pham also supplied the author with a variety of resources for this project. The author thanks Eric Christensen for his input on MMOD and its effects in DSE.

The author would also like to acknowledge DC Space Grant and NASA Office of Education, particularly Dr. Madonna Adams, Heather Ogletree, Carolyn Snyder, and Diego Rodriguez for giving her the opportunity to intern at NASA JSC and assuring that she had a smooth transition. Participating in this research effort and being at JSC has been an extraordinary experience.

[3] Flores, Melissa. Private Conversation. Houston, TX. 25 July, 2012.
[4] Flores, Melissa. Private Conversation. Houston, TX. 25 July, 2012.

References

[1] Accola, A.L., Johnson, G.E., Robbins, R.L., "Designing for On-Orbit Maintenance," IAF-91-091, 1991.

[2]Allen, C.C., Altunin, K.R., Altunin, V.I., Arno, R.D., Bailey, S.G., Balogh, W.R., et al., *Human Spaceflight: Mission Analysis and Design*, Space Technology Series, The McGraw-Hill Companies, Inc., New York, 1999, pp. 116.

[3]Beck, S., Calley, M., Knudsen, J., Kvarfordt, K., Smith, C., Wood, Ted., "SAPHIRE Basics," Idaho National Engineering and Environmental Laboratory, 2005.

[4]Cheng, P., Bohner, J., Hecht, T., "Why Satellites Fail: Lessons for Mission Success," *The Aerospace Corporation Class* [PowerPoint slides], November 17, 2011.

[5]Cheuvront, D.L., "Space Station Freedom Electric Power System Reliability and Maintainability Guidelines Document," Rocketdyne Division, Rockwell International, Canoga Park, CA, 1989

[6]Department of Defense, "Maintainability Design Techniques," DOD-HDBK-791 (AM), 1988.

[7]Gilley, G., "Fault Tolerant Design and Autonomous Spacecraft," 3rd Computers in Aerospace Conference, 1981. Available as AIAA Paper 1981-2170

[8]Hamlin, T., "Human Reliability Analysis Methodology and Modeling Results from Space Shuttle Program," NASA JSC Safety and Mission Assurance [PowerPoint slides], Feburary, 2012.

9Hirsch, R.S., "Crew Systems and On-Orbit Maintainability Design Criteria," Rockwell International Space Station Systems Division., Rept. SSSD-EVA&MS-JAG-87-085, Downey, CA, April 1987.

[10]Kratz, L., "Designing and Assessing Supportability in DOD Weapon Systems: A Guide to Increase Reliability and Reduce Logistics Foodprint," TLCSM Supportability Assessment Guide 10-24-03, Washington, DC, 2003.

[11]Nieberding, J., Ross, L., "Space System Development: Lessons Learned," *Aerospace Engineering Associates LLC Space System Development: Lessons Learned Class Version 3.0 Revision AC* [PowerPoint slides], 2010.

[12]Saleh, J.H., and Castet, J., *Spacecraft Reliability and Multi-State Failures*, 1nd ed., John Wiley and Sons, Ltd., Chichester, United Kingdom, 2011, Chaps. 1, 4 .

[13]Texas A&M University, "STS-117 OMS Pod Blanket Repair Wind Tunnel Testing Interim Summary," [PowerPoint slides], July 29, 2005.

[14]Vesely, W., Stamatelatos, M., Dugan, J., Fragola, J., Minarick III, J., Railsback J., "Fault Tree Handbook with Aerospace Applications," version 1.1, NASA, August 2002.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2015	Technical Memorandum

4. TITLE AND SUBTITLE
Low-Earth Orbit Reliability and Maintainability Paradigms and Their Application to Deep Space Exploration

5. FUNDING NUMBERS

6. AUTHOR(S)
Mariel Rico; Melissa Flores

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Lyndon B. Johnson Space Center
Houston, Texas 77058

8. PERFORMING ORGANIZATION REPORT NUMBERS
S-1195

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
TM-2015-218580

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified/Unlimited
Available from the NASA Center for AeroSpace Information (CASI)
7115 Standard
Hanover, MD 21076-1320 Category: 18

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
As NASA develops more interest within Deep-Space Exploration (DSE), there are a variety of Reliability, Maintainability, and Supportability (RMS) concerns that need to be addressed to lower the risks of loss of crew or loss of mission. Low-Earth Orbit RMS paradigms are no longer valid because of the nature of a Deep-Space (DS) mission. An overview research effort has been put forward to identify RMS practices from past human spaceflight programs, and then re-evaluate and apply them into DSE craft design and processes. Design considerations investigated include general hardware considerations, and the human factors affects on a DS spacecraft. This information will help spacecraft designers prioritize subsystems for maintenance therefore decreasing the likelihood of failures. In the past, maintainability was not as much of a concern because missions were closer to Earth. Temporary fixes were possible because missions were shorter. Resupply missions were possible because of the closer distance; therefore, missing a spare was not as dire. However, temporary fixes during a short-term mission eventually needed to be managed with a more permanent solution. In DSE missions, the opportunity for resupply missions may not be readily available. It is important to implement more efficient RMS standards to overcome these obstacles.

14. SUBJECT TERMS	15. NUMBER OF PAGES	16. PRICE CODE
spacecraft design; aerospace safety; mirometeoroids; cosmic rays; Comet Nucleus Tour; extravehicular activity; telerobotics; risk assessment	18	

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	Unlimited