13-17 July 2014, Tucson, Arizona

Environmental Control and Life Support System Reliability for Long-Duration Missions Beyond Lower Earth Orbit

Miriam J. Sargusingh[1] and Jason R. Nelson[2]
NASA Johson Space Center, Houston, TX 77058

NASA has highlighted reliability as critical to future human space exploration, particularly in the area of environmental controls and life support systems. The Advanced Exploration Systems (AES) projects have been encouraged to pursue higher reliability components and systems as part of technology development plans. However, no consensus has been reached on what is meant by improving on reliability, or on how to assess reliability within the AES projects. This became apparent when trying to assess reliability as one of several figures of merit for a regenerable water architecture trade study. In the spring of 2013, the AES Water Recovery Project hosted a series of events at Johnson Space Center with the intended goal of establishing a common language and understanding of NASA's reliability goals, and equipping the projects with acceptable means of assessing the respective systems. This campaign included an educational series in which experts from across the agency and academia provided information on terminology, tools, and techniques associated with evaluating and designing for system reliability. The campaign culminated in a workshop that included members of the Environmental Control and Life Support System and AES communities. The goal of this workshop was to develop a consensus on what reliability means to AES and identify methods for assessing low- to mid-technology readiness level technologies for reliability. This paper details the results of that workshop.

Nomenclature

AES	=	Advanced Exploration Systems
ARC	=	Ames Research Center
CTSD	=	Crew and Thermal Systems Division
ECLSS	=	Environmental Control and Life Support System
EMAT	=	Exploration Maintainability Analysis Tool
FOM	=	Figure of Merit
JSC	=	Johnson Space Center
LEO	=	Low-Earth Orbit
LRC	=	Langley Research Center
PRA	=	Probabilistic Risk Assessment
RAM	=	Reliability, Availability, Maintainability
RBD	=	Reliability Block Diagram
S&MA	=	Safety and Mission Assurance
SME	=	Subject Matter Expert
TIM	=	Technical Interchange Meeting
TRL	=	Technology Readiness Level
WRP	=	Water Recovery Project

I. Introduction

As part of NASA's Advanced Exploration Systems (AES) program, the AES Water Recovery Project (WRP) is pioneering new approaches for rapidly developing and testing prototype systems in an effort to increase the reliability of water recycling for deep space human exploration missions.[1] Per the NASA Strategic Space

[1] Systems Engineer, Crew and Thermal Systems Division, 2101 NASA Parkway/EC3.
[2] Human Resources Development Specialist, Human Resources Development Branch, 2101 NASA Parkway/AH3.

Technology Investment Plan, "Reliability, logistics, and loop closure of spacecraft environmental controls and life support systems (ECLSS) all contribute to overall mission lifecycle costs and opportunities; the more reliable and resource-efficient an ECLSS is, the farther a mission can safely travel from Earth (and from the option of resupply) and the less mass will have to launch, saving significant costs."[2]

In keeping with this charter, NASA intended for reliability to be a key Figure of Merit (FOM) in an effort to establish a reference architecture for the AES Water Recovery System, which would serve to guide future technical planning, establish a baseline development roadmap for technology infusion, and establish baseline assumptions for an integrated ground and on-orbit life support systems definition.[3] The reliability FOM was initially based on qualitative assessment of each system for reliability indicators such as number of moving parts and number of uniquely controlled elements. This FOM was not accepted by the project stakeholders, nor was an alternative FOM supplied. Upon further evaluation, two challenges to acquiring a reliability FOM became apparent:

1. The AES WRP stakeholders held different understandings of "reliability."
2. There were insufficient data on the low- to mid-Technology Readiness Level (TRL) technologies being developed by WRP to support traditional reliability analysis.

To address these challenges, members of the AES WRP initiated an effort to educate themselves and the entire AES community on concepts and available tools/methodologies associated with reliability. The objectives of this effort were as follows:

1. Develop consensus on a common definition of "reliability" among AES projects.
2. Develop a consensus on how AES projects will assess reliability.
3. Identify the information that must be known about a system to effectively assess its reliability.

It was critical that AES project leadership gain a fundamental understanding of reliability concepts, methodologies, and available tools to meet the objectives. To accomplish this a curriculum was designed that covered selected competencies from NASA's Reliability, Availability, Maintainability (RAM) competency model. The design of this curriculum consisted of an educational series of five short courses that were each 2 hours in length and offered in-person and virtually to AES and ECLSS community members. Subject Matter Experts (SMEs) were identified to lead each of the five courses. This educational series concluded with an "AES Reliability Technical Interchange Meeting (TIM)" where all members of AES and ECLSS communities were invited to participate. The goal of the TIM was to gain a consensus on a common reliability definition and to identify methods for assessing reliability of mid-readiness level technologies.

II. Proceedings

A. Evaluating Systems for Reliability – A Safety and Mission Assurance Perspective

This course, led by members of the NASA JSC Safety and Mission Assurance (S&MA) organization, provided an overarching perspective of "reliability" and assessment tools. To begin, the course leaders highlighted that what most consider reliability is really a three-faceted concept known as RAM The definitions for each element of RAM were given as follows:

- Reliability – the ability of a system to perform its intended function.
- Availability – a characteristic of repairable or restorable items or systems, assumes that a failed item can be restored to operation through maintenance, reconfiguration, or reset.
- Maintainability – the ability to maintain or restore a system function within specified time and effort.

This course included a description and application of tools such as Probabilistic Risk Assessment (PRA), Failure Modes & Effects Analysis (FMEA), Reliability Block Diagrams (RBD), and fault trees. A key takeaway from this course included a realization that a PRA may not be the most appropriate tool for assessing reliability in low- to mid-readiness level systems that have little reliability data available, and RBDs may be useful for faster/low- fidelity assessment of architecture reliability.

B. Accelerated Reliability Testing

Darwin Poritz, a statistician in the JSC Crew and Thermal Systems Division (CTSD), was invited to lead a discussion on accelerated life testing. The objective of this course was to explain the principles that underlie accelerated life testing and to present the rationale for accelerated life testing at NASA. Two examples of accelerated life testing at NASA were presented. The principles behind accelerated testing are based on the work of the Swedish chemist Svante Arrhenius (1859-1927). Life testing is based on the principle that most reactions require an activation energy – an energy barrier that must be overcome before two molecules will react. The idea of accelerated testing is that the more energy that is applied to a system, the more the system ages.

Life testing involves testing a component or system to a key event that is defined by the investigator. This could be a specific kind of failure, any failure, end of useful life, some level of degradation in performance, etc. Accelerated life testing is based on the principle that energy "ages" things and that a particular change occurs at the activation energy. Applying more intense energy will cause the system to reach its activation energy in a shorter amount of calendar time. An example would be to cycle a system at a faster rate than would be experienced during operation (e.g., cycle 1000 times over 2 weeks instead of the 10 years these cycles would normally accumulate.) Long-term reliability will be very important for deep space missions. Accelerated testing may be the only way of simulating long-term stresses over a reasonable time for equipment development and testing on the ground. Reliability testing of multiple items on the ground will likely reduce the number of spares that need to be launched. The idea is to manufacture and test more units on the ground to achieve higher reliability of the units that are launched. Life testing is more common in industries where parts are numerous and inexpensive, and can therefore be tested to failure. Given this, life testing on space systems is a challenge since many systems or system components are unique and are available in very small quantities.

C. Exploration Maintainability Analysis Tool Demo

Representatives from NASA Langley Research Center (LRC) were invited to introduce the concept of supportability and to view a demonstration of the Exploration Maintainability Analysis Tool (EMAT) with modeling and simulation capabilities to assess supportability issues for deep space vehicles. Supportability refers to the inherent characteristics of design and operations that enable the effective and efficient maintenance and support of the spacecraft throughout the mission. Supportability involves a number of design issues, including reliability, reparability, redundancy, sparing, and maintainability. Proposed NASA missions beyond low-Earth orbit (LEO) will introduce these substantial new challenges in the area of supportability and maintainability:

- Limited or no logistics chain back to Earth.
- No quick abort path back to Earth – increases the criticality of spacecraft systems and increases the demands on overall spacecraft reliability.
- High sensitivity of transportation elements to increased logistics mass – very high “gear ratio.”
- Exposure to radiation environment – more difficult to estimate the failure rates of systems and components.

Because of these challenges, a huge level of uncertainty exists in how to design and operate spacecraft for deep space missions. This includes uncertainty in the amount of maintenance and spares that must be manifested on the mission to ensure the safety of the crew and the reliability of the mission. Little or no re-supply occurs during these missions, and there are a large number of critical components and systems. Other design considerations include the ease of access to critical systems and components, volume allocations for spares, consumables, and tools, and time requirements on the crew to maintain and repair systems. The amount of mass and volume that must be committed to spares and maintenance items to assure a safe and effective mission could be a first-order driver in spacecraft and mission design. A perception exists that improved reliability could alone solve the supportability challenges. Although improved reliability should directly reduce required crew time for repair and maintenance mass, improved reliability likely will not directly reduce required spares mass. Manifesting of spares is intended to protect against possible failures, not simply expected failures. Reliability is not the only strategy for solving the supportability challenges on beyond-LEO missions.

Strategies for improving supportability include:

- *Reliability*: Increase the predicted mean time before failure for critical components and systems.
- *Lower Level of Repair*: Provide opportunity and capability for the crew to repair failed equipment at lower levels, replacing only the failed element rather than the entire unit.
- *Redundancy*: As an alternative to repair, provide for backup or degradable capabilities.
- *Commonality*: Design systems to use similar units or repair items.
- *Cannibalization and Asset Reallocation*: Scavenge parts from expired modules prior to jettison or discard to build up spares stock.
- *In-Space Manufacturing*: Provide capabilities to manufacture replacement parts or tools.
- *Repair During Assembly*: Provide for a concept of operations that allows all system failures to be repaired and spares stocks replenished immediately prior to departure to the exploration destination.

Because the maintainability may be a first-order driver in design, it is critical that NASA have a capability to evaluate maintainability for beyond-LEO missions. Because of the new environment and lack of historical data, NASA had no effective capability to evaluate sparing requirements and spacecraft reliability (including repair activities) for such missions. NASA initiated a project to develop modeling and simulation capabilities to assess supportability issues for deep space vehicles. The desired capabilities included:

- Estimate mass/volume of spares and maintenance items

- Predict spacecraft reliability/safety
- Estimate crew time requirements
- Evaluate impacts of system design
- Evaluate effectiveness of strategies to reduce mass/volume requirements and improve reliability
- Possess the ability to trade mass/volume, time, design, and reliability

The initial goal is not necessarily to make absolute estimates of reliability or mass, but rather to explore the design factors that will impact maintainability. A joint NASA/Binera/Georgia Tech University team is currently developing a model to support mission and architecture analysis that investigates supportability for beyond-LEO missions. Using EMAT, the modeler is able to perform a dynamic simulation that functions as a virtual spacecraft. A dynamic simulation includes the following elements:

- Models spacecraft systems, components, and operations using logical relationships.
- Employs a Monte Carlo approach to simulate representative missions with stochastic failures.
- Simulates failures and repairs for a candidate exploration mission.
- Simulates maintenance, failures, and repair actions on key systems in the elements that make up a deep space vehicle.
- Tracks the actions and materials required to maintain and repair the systems.
- Evaluates the overall reliability of the systems based on the supportability.

D. Statistical Analysis for Assessing Reliability

Mark Powell, a consultant with specialization in systems engineering and risk assessment, led the next seminar. He focused the discussion on dealing with engineering specialties associated with the "-ilities"; i.e., requirements that define design aspects with the "-ility" suffix such as reliability, availability, etc. He proposed that all "-ilities" address uncertain performance and have the following common key characteristics:

- states a required probability of performance (by definition)
- establishes a maximum acceptable risk
- covers a specified period of performance

From this perspective, the following definitions were provided to supplement those provided by the S&MA organization (defined in Section II. A. herein):

- *Reliability*: probability that item will survive (not fail before) to a specified service life
- *Availability*: the probability that the item will be in a condition and state ready to perform intended function when called upon during a specific service life
- *Maintainability*: probability item can be repaired in some period of time
- *Logistics*: probability that a part needed to repair can be provided within some period of time
- *Safety*: probability that no harm or injury will occur within some period of time
- *Quality*: probability that part meets requirements

Mr. Powell led a discussion on the difficulties of dealing with "-ility" requirements while engineering systems. He presented several challenges including: complexity and non-inituitive nature of probability and statistics theory, the interrelated nature of the "-ilities," complexity associated with decomposition and allocation of probability and performance to base elements in complex systems, and verification that requires a significant amount of testing and analysis to acquire a "probability that a probability was satisfied by the as-built."[4] During this conversation, it was highlighted that there exists a human element that makes probabilistic analysis difficult to comprehend and apply to decision making. It was noted that decision analysis involves not only the probability of an event occurring, but the value we place on the possible outcomes.

Mr. Powell provided some basic advice for dealing with engineering specialties, as well as an overview of some advancements in probabilistic risk assessment. Of particular interest was the use of objective models of uncertainty in pre-posterior distributions through the use of the Markov Chain Monte Carlo method. This method is appealing due to its applicability to systems that lack data because they have not yet been built, which is typical of the system being developed by AES.

E. Safety and Mission Assurance Rapid Response Risk Assessment Tool

The objective of this course was to introduce and demonstrate the Rapid Response Risk Assessment (R3A) Tool. The R3A tool was developed by the JSC S&MA analysis team to quantitatively assess safety and mission success risks of missions and projects in a timely manner. This tool integrates several capabilities:

- EC Tree, an Excel-based tool and method to rapidly develop event trees and assess the probability of successfully meeting mission goals

- Mission Event Risk Evaluation Models and Library to evaluate and quantify risk of events and systems associated with alternative mission scenarios
- System/Function Reliability Tool and Library
- Extensive system component, subsystem and event reliability and risk data bases

This interactive, real-time mission reliability and risk assessment tool allows a project designer to assess the impact of alternative design options on the probability of mission success. The tool supports mission modeling and offers risk trades for design characteristics, including component reliability characteristics, functional redundancy levels, and alternative mission event characteristics. The tool provides a rapid-response quantitative safety and mission success risk assessment capability for identifying and comparing system and mission risk areas in the early acquisition phases (conceptual and very early design phases).

F. Johnson Space Center Advanced Exploration Systems Reliability Workshop

This workshop included representatives from various AES project and personnel with expertise in ECLSS operations and development, and statistical analysis. A statement defining the AES reliability objective was crafted from this workshop. The statement reads: The goal of AES is to identify and develop technologies that have inherent reliability and potential to improve overall system reliability, and to operate our systems in relevant envrionments so as to identify and address weaknesses.

Various methods for evaluating systems against this objective were identified and organized on a PICK chart[5], a Lean Six Sigma tool adapted for this workshop as a decision grid to organize ideas and select the best ones to implement. Ideas on how technologies may be evaluated for reliability generated generated by the workshop participants and collectively placed on the 2x2 grid based on the payoff on the vertical axis and difficulty to implement on the horizontal. Difficulty would typically include some assessment of cost to implement where more expensive actions can be said to be more difficult to implement. The acronym comes from the labels for each of the quadrants of the grid: Possible (easy, low payoff), Implement (easy, high payoff), Challenge (hard, high payoff), and Kill (hard, low payoff). The quadrant in which an idea falls guides the action associated with that idea. Implement and Kill are obviously stated. Items listed in the "Possible" column might be considered for very quick "back of the envelope" trades. Items in the upper right "Challenge" quadrant require more resources to implement; these mightbe more effective for higher TRL technologies where more data exists to support such analyses.

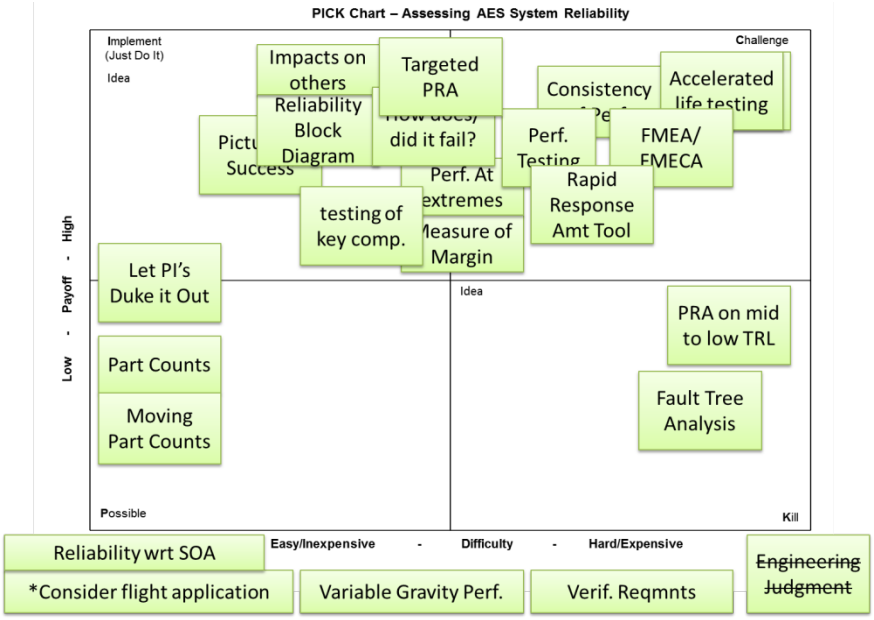

Figure 1. AES Reliability Workshop resultant PICK chart. *Depicts ideas for evaluating AES technologies for reliability plotted on a PICK chart. Items not excluded from the plot were not considered valid evaluation methods.*

The resultant electronic PICK chart is shown in Figure 1. Some ideas shown in the figure were not plotted. "Engineering Judgement" was considered to be inherent to any reliability analysis; particularly for low to mid-TRL technologies. The remainder of the unplotted items were submissions that served more as points of consideration than as evaluation techniques:

- Reliability of a technolgoy as compared to the State of the Art (SOA) technologies
- How the technology would be implemented in flight
- Performance of the technology in variable gravity environments
- Requirements verification

Per the resultant chart and discussion, AES project representatives might consider the following evaluation techniques to obtain early indication of system reliability:

1. Defining the "picture of success," then evaluating the conceptual system against that picture
2. Conducting focused testing on key components of the system
3. Developing a Reliability Block Diagram
4. Evaluating the impact of the system operations and failures on other systems
5. Performing a targeted probabilistic risk assessment
6. Categorizing how the system fails
7. Testing system performance at the extremes of its expected operation
8. Evaluating the performance margin available in the system

III. Conclusion

Prior to the Reliability Education Series, varied understandings of reliability made development of trade study FOMs and specific technology development goals and objectives difficult to define. This series provided the AES and ECLSS communities with a common lexicon with which to communicate. Instead of defining reliability, this series provided additional terms for attributes that the collective community associates with reliability. These terms include: reliability, availability, maintainability, sustainability, etc. Additionally, the series defined various tools that would aid in evaluating systems for reliability and their applicability with respect to complexity and maturity of the technology. Many systems being developed within AES would benefit from analysis tools that do not require detailed systems definition or a significant amount of test data such as RBDs. Additionally, when evaluating mission architectures one might considering using the Rapid Response Risk Assessment Tool and/or EMAT developed by JSC S&MA organization and LRC, respectively.

Ultimately, use of any specific tool or technique would be dependant on the specific technology, the amount of data available, and the budget and schedule resources available for implementing the technique. While the Reliability Education Series provided for an initial discussion on the topic, development of a specific reliability FOM for the WRP reference architecture development remains forward work.

Acknowledgments

The authors would like to acknowledge the SMEs Mark Powell of Attwater Consulting, Darwin Porwitz of JSC CTSD, Christine Stewart and Roger Boyer of JSC S&MA, William Cirillo and Kandyce Goodliff of LRC for their support in leading the seminars and final workshop, and Harry Jones of Ames Research Center (ARC) for providing an annotated bibliography on life support reliability. We acknowledge the contributions of Wade Bostick and Sarah Shull for their support in identifying and coordinating the SMEs. Finally, we gratefully acknowledge the participants of the workshop for their contributions and insight: Layne Carter of Marshall Space Flight Center, Barry Epstein at NASA Headquarters, Harry Jones of ARC, and Jordan Metcalf, Molly Anderson, Wade Bostick, Sarah Shull, Tony Hanford, Subra Sankara, Kevin Lange, Michael Callahan, Kriss Kennedy, Michael Ewert, Karen Pickering, Lisa Erickson, Nik Adam, Denise Varga, Stuart Pensinger, Julie Mitchell, Dan Barta and Jim Broyan of JSC, in addition to the aforementioned SMEs.

References

[1]"About Advanced Exploration Systems (AES)". NASA. Ed. Sarah Loff. NASA, 19 Feb. 2013. Web. 25 Feb. 2014. <http://www.nasa.gov/directorates/heo/aes/>.

[2]NASA Strategic Space Technology Investment Plan. NASA, 13 Dec. 2013. Web. 25 Feb. 2014. <http://www.nasa.gov/offices/oct/home/sstip.html>.

[3]Sargusingh, M. J., "Advanced Exploration Systems Water Architecture Study Interim Results," *AIAA International Conference on Environmental Systems*, Chapter DOI: 10.2514/6.2013-3384, Houston, TX, 2013.

[4]Powell, M. "Dealing with the Engineering Specialties." *Attwater Consulting - Tutorial and Seminar Presentations*. Attwater Consulting, 20 Mar. 2013. Web. 25 Feb. 2014. <http://attwaterconsulting.com/TutSEmPres.htm>.

[5]Carreira, Bill, and Bill Trudell. L*ean Six Sigma That Works: A Powerful Action Plan for Dramatically Improving Quality, Increasing Speed, and Reducing Waste*. New York: American Management Association, 2006. Print.