13-17 July 2014, Tucson, Arizona

ECLSS 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

Reliability has been highlighted by NASA 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, there is no consensus on what is meant by improving on reliability; nor 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 (WRP) hosted a series of events at the NASA Johnson Space Center (JSC) with the intended goal of establishing a common language and understanding of our reliability goals and equipping the projects with acceptable means of assessing our 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 evalauating and designing for system reliability. The campaign culminated in a workshop at JSC with members of the ECLSS and AES communities with the goal of developing a consensus on what reliability means to AES and identifying methods for assessing our low to mid-technology readiness level (TRL) technologies for reliability. This paper details the results of the workshop.

Nomenclature

AES	=	Advanced Exploration Systems
WRP	=	Water Recovery Project
ECLSS	=	Environmental Control and Life Support Systems
RAM	=	Reliability, Availability, Maintainability
FOM	=	Figure of Merit
TRL	=	Technology Readiness Level
WRS	=	Water Recovery System
ELC	=	Embedded Learning Consultant
RAM	=	Reliability, Availability, Maintainability
SME	=	Subject Matter Expert
TIM	=	Technical Interchange Meeting
PRA	=	Probabalistic Risk Assessment
FMEA	=	Failure Modes & Effects Analysis
RBD	=	Reliability Block Diagram
MTBF	=	Mean Time Before Failure
EMAT	=	Exploration Maintainability Analysis Tool

I. Introduction

As part of NASA's Advanced Exploration Systems (AES) program, the AES Water Recovery Project 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 Technology Investment Plan, “Reliability, logistics, and loop closure of spacecraft environmental controls and life

[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.

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, reliability was intended to be a key figure of merit (FOM) in an effort to establish a reference architecture for AES Water Recovery System (WRS) which would serve to guide future technical planning, establish a baseline development roadmap for technology infusion, and establish baseline assumptions for 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 was 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, the AES Water Recovery Project initiated an effort to educate itself and the entire AES project community on concepts and available tools/methodologies associated with reliaiblity. A key to this approach was the inclusion of a highly experienced training and development professional, from the NASA Johnson Space Center Human Resources Development Office, who served as an embedded learning consultant (ELC) and was a key member of the project team. The learning solution design and proceedings are offered in this report.

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

II. Learning Solution Design and Development

To meet these objectives, it was critical that AES project leadership gain a fundamental understanding of reliability concepts, methodologies, and available tools. To accomplish this, the ELC and WRP Systems Engineering and Integration Lead designed a curriculum that covered selected competencies from NASA's Reliability, Availability and Maintainability (RAM) competency model. The design of this curriculum consisted of an educational series of five short courses that were 2 hours in length each and offered in-person and virtually to AES and ECLSS community members. The ELC identified subject matter experts (SME) for each of the five courses and worked with the SME to design training that targeted the aforementioned competencies and objectives. 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.

III. Proceedings

A. Evaluating Systems for Reliability - An S&MA Perspective

This course, lead by members of the NASA Johnson Space Center Safety and Mission Assurance organization, provided an overarching perspective of "reliability" and assessment tools. To start the course, it was highlighted that what most consider reliability is really a three-faceted concept known as RAM (Reliability, Availability, Maintainability). 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 Probability 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 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 RBD 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, 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. A key event 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 two 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 to test more units on the ground in order 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. Langley Exploration Maintainability Analysis Tool (EMAT) Demo

Representatives from NASA Langley Research Center (LRC) were invited to introduce the concept of supportability and to view a demonstration of a 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 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, there is a huge level of uncertainty 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 in order to ensure the safety of the crew and the reliability of the mission. There is little or no re-supply 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 in order to assure a safe and effective mission could be a first order driver in spacecraft and mission design. There is a perception that improved reliability could alone solve the supportability challenges. While 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 (MTBF) 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 utilize 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 ConOps that allows all system failures to be repaired and spares stocks replenished immediately prior to departure to the exploration destination

Because it may be a first-order driver in design, it is critical to 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 beyond-LEO missions. NASA initiated a project to develop modeling & 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
- 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 a tool called the "Exploration Maintainability Analysis Tool" (EMAT), the modeler is able to perform a dynamic simulation that functions as a "virtual spacecraft":

- Spacecraft systems, components, and operations are modeled using logical relationships.
- Simulation 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, lead 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 probability, reliability, availaibility, 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 III. 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 proceeded to lead 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 which 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 a human element in responding to probabilistic assessments; decision analysis involves not only the probably of an event occurring but the value we place on the possible outcomes.

Mr. Powell then provided some basic advice for dealing with engineering specialties and provided 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 Markov Chain Monte Carlo method. What is appealing about this method is its applicability to systems that lack data because they have not yet been built; typical of system being developed by AES.

E. S&MA Rapid Response Risk Assessment Tool

The objective of this course was to introduce and demonstrate the "Rapid Response Risk Assessment Tool." This is an interactive, real-time mission reliability and risk assessment tool that 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).

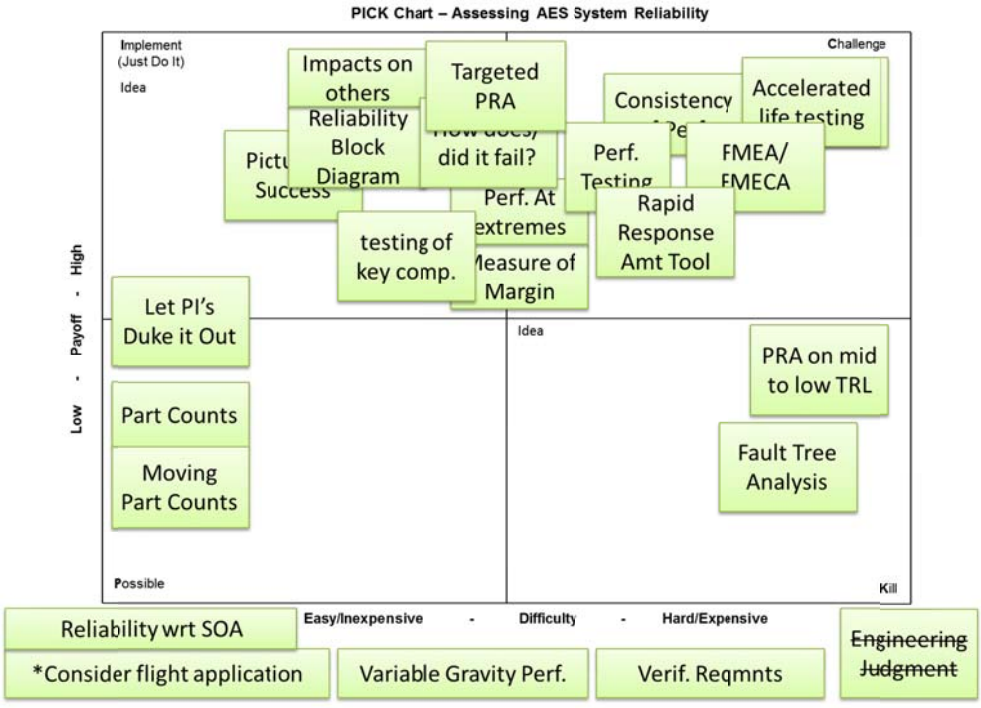
F. JSC AES Reliability Workshop

The workshop included representatives from various AES project and personnel with expertise in ECLSS systems operations and development, and statistical analysis. From this workshop, a statement was crafted defining the AES reliability objective:

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 envrionemnts so as to identify and address weaknesses.

Additionally, various methods for evaluating systems against this objective were identified and organized on a PICK chart. This chart ranks each concept in terms of payoff and difficulty. Per the resultant chart, AES project might consider the following evaluation techniques to get early indication of system reliability:

1. Defining the "picture of success" then evaluating the conceptual system against that picture
2. Focused testing on key components of the system
3. Development of a Reliability Block Diagram
4. Evaluating the impact of the system operations and failures on other systems
5. Performing a targeted probabilistic risk assessment (PRA)
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



IV. Conclusion

Prior to the Reliability Education Series, there were varied understandings of "reliability" making development of trade study FOMs and specific technology development goals and objectives difficult to define. This series

provided the AES and ECLSS community with a common lexicon with which to communicate; instead of defining "reliability", additional terms associated with the attributes the collective community associates with reliability were provided: reliability, availability, maintainability, sustainability, etc. Additionally, various tools were defined 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 Reliability Block Diagrams. 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.

Acknowledgments

(list to be provided in final paper)

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, Mark. "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>.