Improving Reliability and Maintainability (R&M) in Space Life Support

Harry W. Jones[1]
NASA Ames Research Center, Moffett Field, CA, 94035-0001

This paper considers how to improve the reliability and maintainability (R&M) of future NASA space life support systems. If these systems are procured under an industry contract, defining the R&M requirements would take precedence over providing technical guidance on designing the system. Imposing a specific R&M design could be over constraining. However, the mission may define the overall R&M approach, as the International Space Station (ISS) did by requiring Orbital Replacement Units (ORUs). Before defining the R&M requirements for the next mission, the life support research program should understand and plan the R&M approach. The recent NASA technical standard on R&M has moved away from requiring specific R&M activities during each of the traditional project phases to instead developing and planning to implement the R&M requirements to meet the top level project R&M objectives. The emphasis is on providing the evidence to show that the R&M requirements are met, rather than on conducting specific prescribed R&M activities. The technical standard on R&M defines a comprehensive hierarchy of specific R&M objectives and identifies particular strategies to implement them at each level. That is, the top level R&M objective is defined and then one or more design strategies to implement it are developed immediately, before the next lower objectives are defined and the strategies to achieve those are designed. This step-by-step, top-down approach is similar to the axiomatic design method. The objectives are the R&M requirements, and the strategies are the hardware designs or operations plans developed to meet these requirements. The new R&M process is aligned with the systems design process and helps ensure that the methods to meet the R&M requirements are built into the design.

Nomenclature

DOD	=	Department of Defense
FDIR	=	Fault Detection Isolation and Recovery
FMEA	=	Failure Modes and Effects Analysis
FMECA	=	Failure Mode, Effects, and Criticality Analysis
FTA	=	Fault Tree Analysis
GFE	=	Government Furnished Equipment
HALT	=	Highly Accelerated Life Testing
ISS	=	International Space Station
LEO	=	Low Earth Orbit
NPD	=	NASA Policy Directive
NPR	=	NASA Procedural Requirement
ORU	=	Orbital Replacement Unit
PoF	=	Physics of Failure
PRA	=	Probabilistic Risk Assessment
R&M	=	Reliability and Maintainability
RBD	=	Reliability Block Diagram
RCM	=	Reliability Centered Maintenance
SMA	=	Safety and Mission Assurance
STD	=	Standard

[1] Systems Engineer, Bioengineering Branch, Mail Stop N239-8.

Introduction

THIS paper considers how to achieve satisfactory reliability and maintainability (R&M) in NASA's space life support systems. The NASA R&M standard, policies, and requirements are reviewed. The current NASA technical standard on R&M is recent and makes a significant departure from the previous long standing NASA R&M approach. The new R&M standard has general top-level process requirements, but the specific approach to achieving R&M should be tailored to the particular system. Typically, only a few of the many R&M analysis techniques can or should be used in any one project.

I. NASA safety, reliability and maintainability, and human-rating requirements documents

In 2017, after 20 years, NASA issued a major revision of the R&M policy, NASA-STD-8729.1A. Formerly NASA required certain specific R&M activities during every succeeding phase of project development. Now NASA requires a project to start with the initial development of R&M requirements and the devising of strategies to implement and verify them. And rather than doing all the requirements first and then designing the system, as has been usual in systems design, the design process now is to work top down by layers, identifying the top level requirements and suggesting top level design strategies for those, then making these higher strategies the basis for a lower level of requirements, and so on down to the lowest components. This approach is intended to ensure that R&M is designed in from the beginning rather than added with difficulty to a completed design concept. The new R&M standard seems to be the basis of a innovative and effective reliability design approach.

The NASA R&M documents will be shown in a precedence tree and the essential NASA documents described in detail. The document tree is shown in Figure 1.

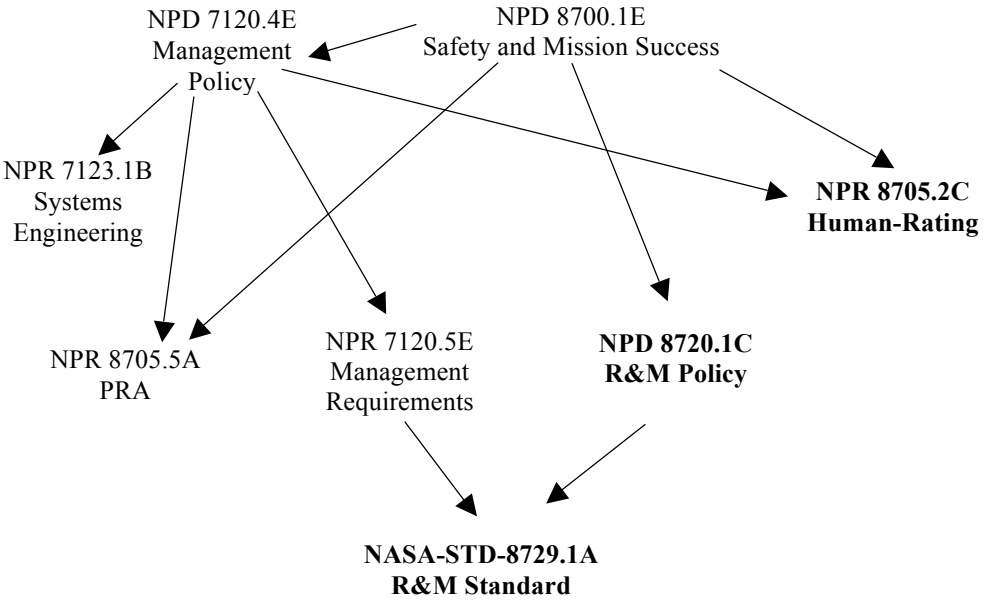

Figure 1. NASA safety, reliability and maintainability, and human-rating document tree

The key operative documents are shown in bold: NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy, NASA-STD-8729.1A, Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems, and NPR 8705.2C, Human-Rating Requirements for Space Systems. They were revised in June and July of 2017. Table 1 is a list of the R&M documents with their full titles and revision dates.

Table 1. Reliability and Maintainability (R&M) document list

Number	Title	Date
NASA-STD-8729.1A	NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems	6/13/2017
NPD 7120.4E	Program/Project Management Policy	6/26/2017
NPD 8700.1E	NASA Policy for Safety and Mission Success	12/6/2013
NPD 8720.1C	NASA Reliability and Maintainability (R&M) Program Policy	4/18/2008, 4/16/2013
NPG 7120.5E	NASA Space Flight Program and Project Management Requirements	8/14/2012
NPR 7123.1B	NASA Systems Engineering Processes and Requirements	4/18/2013
NPR 8705.2C	Human-Rating Requirements for Space Systems	7/10/2017
NPR 8705.5A	Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects	6/7/2010

NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems, is the key NASA R&M document, issued 6/13/2017. The previous NASA-STD-8729.1 was issued 12/1/1998 and was very different. NASA-STD-8729.1A's governing document is NPG 7120.5E, NASA Space Flight Program and Project Management Requirements. The applicable policy directive is NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy.

A. NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy

NASA Policy Directive (NPD) 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy requires a program to "establish, document, and implement" the R&M design and performance requirements, to define the maintenance concepts, requirements, activities, and schedule, and to assess compliance with the R&M requirements. R&M activities include requirements specification, failure mode identification, design validation, data collection, quantitative and qualitative modeling and analysis, and testing and demonstration. Engineering for R&M is a specific but not an isolated activity. The R&M design approach assumes the full system engineering and development process will be carried out and that R&M will be integrated into it. R&M must also be coordinated with risk management, safety, security, quality assurance, logistics, probabilistic risk assessment, life-cycle cost, and configuration management. The R&M requirements should address the availability metric. Guidance on R&M program management is provided in NASA-STD-8729.1, now NASA-STD-8729.1A.

B. NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems

Revision NASA-STD-8729.1A was approved 6/13/2017 and issued 9/6/2017, and it supersedes the baseline 8729.1 of 12/1/1998. The purpose of the standard is to link programs and projects to NASA's top-level R&M objective, which is to satisfy the mission requirements for Safety, Reliability, Maintainability, and Quality over the life cycle. The revision makes a significant change in the NASA R&M approach, reflecting a more results oriented approach to using contracts. NASA has moved away from requiring specific defined R&M activities during the traditional project phases to instead developing and implementing tailored R&M requirements necessary to meet the top level project R&M objectives. The emphasis is on providing the evidence to show the R&M requirements are met, rather than on conducting certain prescribed R&M activities. The revised standard now applies only to new NASA programs and projects, since its methods are intended "to assure reliability is designed and built into systems." (8729.1A, p. 2) The previous revision could also be applied during the later stages of previously started activities.

"The vision in general is to move from a process-based approach to one that is more rooted in the technical objectives of the stakeholders and Centers and is aligned with systems engineering. In other words, this Standard promotes defining requirements with the focus of meeting the defined technical objectives." (8729.1A, p. 3)

As always, the R&M requirements must be verified, either by inspection, testing, demonstration, or analysis, but here an innovative and probably more effective requirements development and verification process is used. Typically, requirements are fully developed hierarchically from the top to lowest level, and then a specific verification method is developed for each requirement at the lowest level. The traditional system design process begins only after all the lowest level requirements are defined.

The new approach of 8729.1A defines a comprehensive hierarchy of R&M objectives and identifies specific strategies to implement them at each level. That is, the top level objective is defined and then one or more strategies to implement it are developed immediately, before the next lower objectives are defined. These strategies are then used to define the next lower level objectives, which are further implemented by their supporting strategies. The objectives are the R&M requirements, and the strategies are hardware designs or operations plans or other activities developed to meet the requirements. The R&M process is aligned with systems design and helps ensure that the methods to meet the R&M requirements are built into the system from the beginning rather than added onto a constraining preliminary design. Axiomatic design is a similar multilevel, step-down, paired requirements and design process that can help rationalize overall system design. (Jones, 2017-82)

The standard includes the broad technical objectives and strategies that impact reliability, but it is not meant to prescribe specific processes. The R&M objectives and strategies can be tailored by spaceflight programs and projects to ensure that R&M is designed and built into systems. The standard uses a matrix to connect specific program or project activities to the risk objectives for different missions, including human flight, class A to D robotics missions, and technology demonstrations. The standard also lists the recommended R&M evidence (including controls, analysis, testing, and inspection) that R&M engineers can use in the planning, execution and evaluation of a program or project over its life cycle. "Mandatory elements of this Standard require programs and projects to use these objectives and strategies during the planning of activities and formulation of requirements." (8729.1A, p. 5)

1. R&M objectives and strategies

The comprehensive hierarchy of R&M objectives and strategies in 8729.1A contains 14 objectives and 49 strategies, and each strategy has suggested evidence needed to validate it. The hierarchy is applicable to all NASA projects, from human space flight to ground systems. The scope of each strategy is indicated for the different types of projects. The R&M objectives and strategies are listed fully below. They are intended to be used to plan and evaluate R&M activities. 8729.1A is a guiding, not prescriptive standard, since not all of its methods are required and additional activities and evidence can be used.

The objectives-hierarchy approach reflects innovative systems thinking and can be used to guide advanced systems engineering approaches, such as Model-Based Systems Engineering, Model-Based Mission Assurance, and assurance case development. (Feather et al., 2016-5543)

2. R&M evidentiary methods

The R&M strategies must be verified, shown to have been implemented, using appropriate evidentiary methods. The 49 strategies in 8729.1A are each provided with suggested evidentiary methods, such as testing, failure analysis, derating, and many others. There are 69 R&M evidentiary methods described in an appendix, including well known reliability analysis methods, maintainability analysis methods, reliability test and evaluation methods, and maintainability test and evaluation methods. Each method is accompanied by a brief synopsis of what it does, why it is used, when it is called for, and when during a program or project it is performed.

3. R&M requirements planning and implementation

8729.1A states that the R&M requirements should be planned and implemented in the Safety and Mission Assurance (SMA) plan required by NPR 7120.5. The SMA plan should address the specific R&M objectives and strategies in 8729.1A.

The R&M requirements and implementation plan should include the following:

1. R&M criteria, including those derived from safety, logistics, etc.;
2. R&M functional requirements and performance objectives that support R&M activities such as quantitative reliability models and Failure Modes and Effects Analysis (FMEA);
3. Design and process standards impacting system reliability;
4. The R&M products that will be used as evidence that the strategies that were implemented and objectives achieved, considering the suggested evidentiary methods in 8729.1A;
5. Any R&M products used for design requirement verification;
6. The strategy for independent evaluation of R&M products and activities.

C. The earlier NASA-STD-8729.1, Planning, Developing, and Managing an Effective Reliability and Maintainability Program

The original NASA-STD-8729.1 was published December 1998. It was developed to provide a centralized source of information for establishing R&M performance-based requirements, design factors, and metrics. It was written toward the end of Dan Goldin's "better, faster, cheaper" era, which substantially deemphasized traditional reliability analysis in NASA. The original provides generic guidance and unlike the revised 8729.1A, was not

mandatory. The original was for use on all new and existing NASA programs, while the revised 8729.1A is for new programs only.

The original 8729.1 emphasized R&M integration with other organizational elements, including Quality Assurance, Human Engineering, Logistics Support, and Project Engineering. The original also emphasized R&M as part of the system acquisition process, with specific activities defined for R&M during formulation, approval, and implementation. This is significantly different from the new emphasis on coherent and seamless implementation of R&M objectives.

The intent of both the original and the revised R&M standard is to implement requirements based, not process based procurement. The 1998 Goldin era original observed, "the new process of holding contractors accountable for their final product transfers much of the cost, risk, and quality responsibility from NASA to the contractor." (8729.1, p. 4-3) The R&M performance requirements are part of the system end item performance specification. (8729.1, p. 8-2)

The original 8729.1 suggests that R&M performance requirements should be included in the system specification, specifically containing:

1. Definition of operating environment,
2. Definition of system failure,
3. The minimum R&M performance requirements, and,
4. Metrics and verification of the R&M performance requirements.

"The most important thing to remember is to state R&M performance requirements in terms of the required results and provide the criteria for verifying compliance, without stating the methods for achieving the results." (8729.1, p. 8-2)

R&M engineering should perform appropriate R&M trade-off studies, such as the following examples:

1. reliability prediction
2. R&M allocation
3. failure modes and effects analysis
4. criticality analyses
5. fault tree analysis
6. worst case circuit analysis
7. maintainability assessment (8729.1, p. 8-4)

A maintainability assessment should include estimates of the Mean Time To Repair (MTTR) for the key components of a system and a review of these key components for crucial maintainability criteria, such as the following examples:

1. accessibility
2. interchangeability
3. failure detection
4. failure isolation
5. special tools and diagnostics
6. spares
7. logistics support sources (8729.1, p. 8-5)

The essential difference between 8729.1 and the revised 8729.1A is that the original aimed more directly to define the contractor R&M requirements while the revision works at an earlier, higher, and broader systems level to develop an overall plan that addresses the defined R&M objectives by implementing specific strategies. The revised standard encourages an initial design emphasis on achieving R&M goals, and makes it less likely that unexpected R&M difficulties will be discovered later in development. The R&M evidentiary methods and strategies in 8729.1A include and expand the similar R&M toolsets in 8729.1.

D. NPR 8705.2C, Human-Rating Requirements for Space Systems

NPR 8705.2C, Human-Rating Requirements for Space Systems, is mandatory. Its purpose is to define and implement the requirements, procedures, and processes needed to produce safe human-rated space systems. Human-rating activities track the project phases and are an integral part of program activities throughout the system life cycle.

Crewed space systems must obtain a Human-Rating Certification. Verification of human rating requirements is performed by development of products for the milestone reviews (System Requirements Review, System Definition Review, Preliminary Design Review, Critical Design Review, System Integration Review, and the Operational Readiness Review).

Throughout design and development, program management is responsible to ensure that the system works and is safe. The Human-Rating Certification Process is based on certification requirements that lead the program manager through the steps of human-rating and document the results in a Human-Rating Certification Package. The Technical Authorities (Safety, Engineering, and Health and Medical) challenge the developers to defend their design decisions and help identify hazards and provide safer alternatives. Achieving the highest possible safety requires a mindset where each person feels personally responsible for their piece of the design and for the safety of the crew.

The program manager is required to implement and document in the Human-Rating Certification Package, a process for identifying hazards, quantifying and ranking risks to crew safety, and mitigating risks and deficiencies. Commonly used safety and reliability tools include Hazard Analyses, Fault Tree Analyses, Failure Modes and Effects Analysis, Damage Modes and Effects Analysis, Critical Items Lists, Probabilistic Risk Assessment (PRA), and Human Error Analysis. These are also used in Reliability and Maintainability (R&M) analysis.

The human rating requirement to plan the crew workload includes planing for maintenance. A specific human rating requirement is for human error analysis.

NPR 8705.2C is very similar to the earlier revision B. The newer NPR 8705.2C quotes and adds paragraph references for the Human-Rating Certification Package requirements and also changes the Human-Rating Certification form and its endorsement form.

II. The R&M objectives and strategies from NASA-STD-8729.1A

The complete R&M objectives and strategies from NASA-STD-8729.1A are given and discussed below. The top objective and the four major subobjectives are given first, then each subobjective is fully expanded. The outline numbers correspond to the index identification numbers in 8729.1A.

A. Top objective: system performs as required over the lifetime to satisfy mission requirements

The overall purpose of R&M is to ensure the "Top objective: system performs as required over the lifetime to satisfy mission requirements." Unlike system operational performance, which can be verified by a one-time test, R&M is a continuing concern throughout the system's life. The top objective has four subobjectives;

1. Subobjective 1: The system conforms to the design intent and performs as planned.
2. Subobjective 2: The system remains functional for the intended lifetime, environment, operating conditions, and usage.
3. Subobjective 3: The system is tolerant to faults, failures, and other anomalous internal and external events.
4. Subobjective 4: The system is designed to accommodate an acceptable level of availability and maintenance demands.

B. Subobjective 1: The system conforms to the design intent and performs as planned

This "Subobjective 1: The system conforms to the design intent and performs as planned," expands on the top objective's "system performs as required." The full intended performance is required. The strategies to meet Subobjective 1 are defined, with their subobjectives and the corresponding lower level strategies.

1. Subobjective 1: The system conforms to the design intent and performs as planned.
   - 1.A. Strategy: Verify and validate nominal functionality
     - 1.A.1. Objective: Nominal functionality at each level of the system has been verified and validated.
       - 1.A.1.A. Strategy: Demonstrate that the functionality of the system meets the design intent.
   - 1.B. Strategy: Test and inspect adequately to identify and resolve faults, issues, and defects.
     - 1.B.1. Objective: Faults, defects, or other latent issues have been found as part of the testing/inspection process.
       - 1.B.1.A. Strategy: Test, inspect, and demonstrate to ensure that issues have been found.
       - 1.B.1.B. Strategy: Identify cause of anomalies.
     - 1.B.2. Objective: All issues resolved or closed out to an acceptable level of risk.
       - 1.B.2.A. Strategy: Track, address, and trend issues via a closed loop problem resolution process.
   - 1.C. Strategy: Achieve high level of process reliability.
     - 1.C.1. Objective: Built system and its components do not contain flaws/faults that reduce reliability.
       - 1.C.1.A. Strategy: Select appropriate quality components and materials.

1.C.1.B. Strategy: Perform process reliability reviews to ensure consistency of reliability design processes.
1.C.1.C. Strategy: Establish and verify manufacturing processes and handling criteria.
1.C.1.D. Strategy: Screening, proof testing, and acceptance testing.

Strategy 1.A corresponds to the usual performance or acceptance testing, which is not usually considered part of R&M but verifies the performance baseline. Strategy 1.B seems to anticipate that all faults and issues will be resolved, which is not possible. A long life or preflight test would be helpful, with the recommended fault analysis and redesign as needed. Fault tracking and resolution would continue into operations and then become part of the R&M process. Strategy 1.C is applied earlier, during design and manufacturing, but again the "no flaws" is not possible.

Subobjective 1 is concerned with design, test, and early fault correction. These largely establish the system reliability.

C. Subobjective 2: The system remains functional for the intended lifetime, environment, operating conditions, and usage

The "Subobjective 2: The system remains functional for the intended lifetime, environment, operating conditions, and usage," expands on the top objective's "over the lifetime." The full intended system life is required.

2. Subobjective 2: The system remains functional for the intended lifetime, environment, operating conditions, and usage.
   2.A. Strategy: Understand failure mechanisms, eliminate and/or control failure causes, degradation and common cause failures, and limit failure propagation to reduce likelihood of failure to an acceptable level.
      2.A.1. Objective: System and its elements are designed to withstand nominal and extreme loads and stresses for the life of the mission.
         2.A.1.A. Strategy: Apply design standards to incorporate margin to account for variable and unknown stresses.
         2.A.1.B. Strategy: Evaluate and control nominal stresses and related failure causes.
         2.A.1.C. Strategy: Evaluate and control potential for extreme stresses and related failure causes.
         2.A.1.D. Strategy: Perform qualification testing and life demonstration to verify design for intended use.
      2.A.2. Objective: System or its elements are not susceptible to common cause failures.
         2.A.2.A. Strategy: Evaluate and control coupling factors and shared causes between redundant or dependent components.
   2.B. Strategy: Assess quantitative reliability measures and recommend or support changes to system design and/or operations.
      2.B.1. Objective: System and its components meet quantitative reliability criteria.
         2.B.1.A. Strategy: Determine reliability allocation.
         2.B.1.B. Strategy: Estimate reliability based on applicable performance data, historical data of similar systems, and/or physics-based modeling.
         2.B.1.C. Strategy: Support design trades based on reliability analysis.
         2.B.1.D. Strategy: Plan and perform life testing.
         2.B.1.E. Strategy: Track and monitor reliability performance over time.

Strategy 2.A is to eliminate or control failure causes, including excessive stresses, degradation, common cause failures, and coupling and failure propagation. Note that Strategy 2.A.1.D, qualification and life testing, is similar to the testing in 1.B.1.A, 1.C.1.D, and 2.B.1.D. The same testing can meet several different objectives.

Strategy 2.B is to assess, estimate, design, and test for reliability so as to meet the reliability requirement. The usual straight forward project flow is not reflected in the new objectives based approach.

D. Subobjective 3: The system is tolerant to faults, failures, and other anomalous internal and external events

The "Subobjective 3: The system is tolerant to faults, failures, and other anomalous internal and external events," implicitly assumes that not all faults, failures, and anomalous events can be prevented. Strategies and plans to mitigate them are required.

3. Subobjective 3: The system is tolerant to faults, failures, and other anomalous internal and external events.

3.A. Strategy: Assure that system includes necessary barriers and mitigations to keep anomalous events from compromising ability to meet mission objectives.
  3.A.1. Objective: System has multiple means of accomplishing functions that are critical to mission operations including safety.
    3.A.1.A. Strategy: Provide similar or dissimilar redundancy.
  3.A.2. Objective: Physical and functional pathways for fault propagation are limited.
    3.A.2.A. Strategy: Separate redundant paths functionally and physically.
    3.A.2.B. Strategy: Isolate and contain faults.
    3.A.2.C. Strategy: Evaluate and control shortest path to worst case effects (e.g., hazardous events)
  3.A.3. Objective: System is able to recover from anomalies affecting functions that are important to top-level expectations.
    3.A.3.A. Strategy: Provide fault management (detection, active isolation, recovery) capabilities
  3.A.4. Objective: System can degrade or lose functions without significantly impacting top-level expectations (through contingency operations).
    3.A.4.A. Strategy: Plan contingency or other off-nominal operations.

Perfect reliability is not possible. Fault tolerance is needed. Strategy 3.A requires barriers and mitigations, including redundancy, fault isolation and recovery, gentle degradation, and contingency plans. Deciding what and how much is appropriate requires careful cost-benefit and risk calculations.

E. Subobjective 4: The system has an acceptable level of maintainability and operational availability

The "Subobjective 4: The system has an acceptable level of maintainability and operational availability," is concerned with how difficult the system is to maintain and if the system's up time will be sufficient. The use of the word "acceptable" is a reminder that in an operational situation, the users often must do more maintenance and accept less service than they had originally expected.

4. Subobjective 4: The system has an acceptable level of maintainability and operational availability.
  4.A. Strategy: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands.
    4.A.1. Objective: Maintenance and repair activity can be performed within available resources (cost, time).
      4.A.1.A. Strategy: Design to facilitate on-orbit and ground maintenance and check-out.
      4.A.1.B. Strategy: Design to minimize maintenance complexity for reduction of maintenance time and training requirements.
      4.A.1.C. Strategy: During design, consider tool selection, stowage, ease of use, and criticality as well as complexity of robotic maintenance capability where feasible.
      4.A.1.D. Strategy: Use standardization to limit the number of feasible design options and encourage the use of common items. Procedures, tools, etc.
      4.A.1.E. Strategy: Perform RCM (on orbit/ground support systems) during design to optimize the design for maintainability.
      4.A.1.F. Strategy: Perform maintainability simulation and analysis as needed to support design and logistic support analysis.
      4.A.1.G. Strategy: Provide demonstration testing to verify "detect, diagnose, isolate" capability of systems and confirm corrective and preventative maintenance task actions and analysis.
    4.A.2. Objective: System provides clear indication of health status, degradations, and diagnostic information.
      4.A.2.A. Strategy: Identify and optimize the testability and diagnostics to support the maintainability requirements.
      4.A.2.B. Strategy: Incorporate fault/detection/isolation/recovery at the lowest practical level to support the maintainability requirements.
      4.A.2.C. Strategy: Develop test-point design strategies to minimize access time and system intrusion
      4.A.2.D. Strategy: Design in self diagnostics for assemblies to minimize maintenance/recovery time and false alarms.
    4.A.3. Objective: System design allows for reconfiguration, upgrade, or growth opportunities during the mission.
      4.A.3.A. Strategy: Design the system to accommodate future technology or changes in application over the design life via maintenance activities.

4.A.3.B. Strategy: Design for physical and functional interchangeability with other like components and assemblies in the system.

4.A.3.C. Strategy: Incorporate modular designs to facilitate remove-and-replace maintenance and allow flexibility in the design.

4.A.4. Objective: Maintainability performance is validated and optimized during operation based on available maintenance data.

4.A.4.A. Strategy: Establish capabilities and processes to collect and store operational history, health status, degradation, diagnostic, and maintenance data.

4.A.4.B. Strategy: Periodically analyze test and operational history, health status, degradation, diagnostic, and maintenance data to determine maintainability performance and trends.

4.A.4.C. Strategy: Periodically review and update maintenance strategy and activities.

4.A.4.D. Strategy: Ensure the availability of data to future programs and projects.

The overall strategy, 4.A, mentions only the need to "evaluate, control, and monitor" maintenance, but objective 4.A.1 requires design, simulation, and demonstration of maintenance. Objective 4.A.2 requires status, testability, and diagnostics, and even FDIR (fault/detection/isolation/recovery). 4.A.3 requires reconfiguration and upgrade capabilities. 4.A.4 requires gathering, analyzing, storing, and sharing maintenance data.

F. The application of the R&M evidentiary methods

A set of tables in Appendix B of 8729.1A suggests the appropriate evidentiary methods to verify each of the above 49 strategies, such as test, modeling, and analysis or using processes such as derating and part screening. The appendix also explains how the evidentiary methods should be applied in human spaceflight. These evidentiary methods are useful suggestions but are not specifically required.

G. The list of the R&M evidentiary methods

Appendix C describes the 69 R&M evidentiary methods. Each method has a summary of what it does, why it is used, and when it is needed. The evidentiary methods are described under five headings: reliability analysis methods, maintainability analysis methods, reliability test and evaluation methods, maintainability test and evaluation methods, and technical review methods. The evidentiary methods are listed next:

1 Reliability Analysis Methods
- 1.1 Alert Reporting
- 1.2 Approved Parts List
- 1.3 Availability Analysis
- 1.4 Human Error Risk Assessment
- 1.5 Human Factors Task Analysis
- 1.6 Deep Dielectric Charging & Internal Electrostatic Discharge
- 1.7 Failure Mode and Effects (& Criticality) Analysis (FMEA/ FMECA)
- 1.8 Fault Tree Analysis (FTA)
- 1.9 Ground Handling Analysis
- 1.10 Limited-Life Item Analysis
- 1.11 Micro Meteoroid/ Debris Analysis
- 1.12 Parts Control Plan
- 1.13 Parts Traceability
- 1.14 Part Electrical Stress Analysis
- 1.15 Physics of Failure Analysis
- 1.16 Reliability Assurance Plan
- 1.17 Reliability Modeling (Prediction /Allocation)
- 1.18 Reliability Tradeoff Studies
- 1.19 Single Event Effects Analysis
- 1.20 Sneak Circuit Analysis
- 1.21 Structural Stress Analysis
- 1.22 Surface Charging/ESD Analysis
- 1.23 Thermal Analysis of Electronic Assemblies to the Part Level
- 1.24 Thermal Stress/Fatigue Analysis
- 1.25 Trend Analysis
- 1.26 Worst Case Analysis

2 Maintainability Analysis Methods
- 2.1 Link Analysis
- 2.2 Logistics Support Analysis/Plan
- 2.3 Maintainability Modeling (Prediction / Allocation)
- 2.4 Maintenance Concept
- 2.5 Maintenance Engineering Analysis
- 2.6 Maintenance Plan
- 2.7 Reliability Centered Maintenance
- 2.8 Testability Analysis
- 2.9 Tradeoff Studies

3 Reliability Test and Evaluation Methods
- 3.1 Acoustics Test
- 3.2 Constant Acceleration Test
- 3.3 Electromagnetic Compatibility Emissions Test
- 3.4 Electromagnetic Compatibility Isolation Test
- 3.5 Electromagnetic Compatibility Susceptibility Test
- 3.6 Environmental Stress Screening
- 3.7 Electrostatic Discharge Test
- 3.8 Ground Handling Test
- 3.9 Highly Accelerated Life Test
- 3.10 Highly Accelerated Stress Test
- 3.11 Life Testing
- 3.12 Magnetic Test
- 3.13 Mechanical Shock Test
- 3.14 Powered-On Vibration Test
- 3.15 Problem Failure Reporting
- 3.16 Pyrotechnic Shock Test
- 3.17 Random Vibration Test
- 3.18 Reliability Demonstration
- 3.19 Reliability Growth Test
- 3.20 Reliability Test Program Plan
- 3.21 Root Cause Analysis
- 3.22 Sine Burst Test
- 3.23 Sine Dynamic (Sinusoidal Vibration) Test
- 3.24 Structural Proof Loading Test
- 3.25 Thermal Cycling Test
- 3.26 Thermal Shock Test
- 3.27 Thermal Test
- 3.28 Voltage / Temperature Margin Test

4 Maintainability Test and Evaluation Methods
- 4.1 Maintainability Demonstration
- 4.2 Problem Failure Reporting
- 4.3 Root Cause Analysis
- 4.4 Reliability Centered Maintenance

5 Technical Review Methods
- 5.1 Detailed Technical Reviews
- 5.2 Launch Readiness Review
- 5.3 Monitor/Control of Suppliers
- 5.4 Pre-Ship Review
- 5.5 Reliability Audits
- 5.6 Subsystem Inheritance Review

III. Developing the R&M plan

This section describes how to develop an R&M plan. It is based on a particular broad survey and includes best practices and lessons learned.

A. Best practices in R&M plans

The R&M plan should focus on the best practice tasks for providing highly reliable and maintainable systems. The plan should not present a long list of all the possible strategies and evidentiary methods since there are very many and they should be selected and tailored by the project. There are three high level steps to developing the R&M plan:

1. Establish the reliability and maintainability concept or vision.
2. Select the most effective and applicable "best practice" tasks out of the dozens of potential reliability methods and strategies.
3. Identify potential problems that may block achieving the R&M vision. (Carlson et al., 2010)

A partial list of best practices can be identified at each stage of system development. In the concept stage the system level reliability and maintainability requirements are developed and then flowed down to the subsystems and components. Then a Reliability Block Diagram (RBD) can be generated and a system Failure Modes and Effects Analysis (FMEA) developed. The most critical components and subsystems for R&M should be identified. (Carlson et al., 2010)

The design stage must emphasize initial design for reliability and maintainability, since testing and correcting problems found during testing requires much more time and money and since an unconsidered initial design may be incapable of achieving the R&M goals. The design stage best practices include design margin analysis, detailed lower level design, component, and process FMEAs, root cause analysis of known reliability problems, and specific robust design tasks such as physics of failure (PoF) modeling and Highly Accelerated Life Testing (HALT). (Carlson et al., 2010)

The best practice reliability tasks in the testing stage include planning reliability test methods, developing accelerated life test methods, conducting the reliability test plan, and conducting reliability growth testing. (Carlson et al., 2010)

Some common problems in executing R&M plans and in achieving the R&M goals are:

1. Lack of test time.
2. Lack of management support.
3. Lack of understanding of reliability.
4. Lack of learning from test failures. (Carlson et al., 2010)

B. Lessons learned

The potential problems in achieving satisfactory reliability and maintainability include lessons learned from experience:

1. Focus on the few key reliability and maintainability methods needed to achieve the objectives. There are several dozens of reliability methods that could be used.
2. Emphasize reliability tasks that achieve reliability as early as possible in the development process. The earlier that changes are made, the less costly they are.
3. Emphasize methods to design for reliability rather than perform reliability analysis. There are many tools and practices that can help increase the reliability of systems.
4. Safety first. Safety goals and problems must be treated separately from and more rigorously than R&M objectives.
5. Management must be seriously involved, from beginning to end, during the R&M program.
6. Successful execution of the R&M plan requires management buy-in, adequate resources, reviews of progress, and active problem solving.
7. Every project team member should have a defined responsibility for R&M.
8. Management should provide expert reliability engineering support as well as software, training, and technical guidelines. (Carlson et al., 2010)

IV. Reliability and maintainability (R&M) issues in space life support

The R&M review and analysis raised some high level issues that will govern the implementation of R&M in future life support. These considerations are discussed in the following sections.

A. Advanced space life support will probably have R&M problems

Current manufactured consumer products such as electronics and automobiles have high quality, high reliability and maintainability. It was not always so. Automobiles were noted for planned obsolescence, arbitrarily changing styles, and intentionally limited life. Achieving high quality required long and intense efforts before much improvement was seen. Military systems have lower than commercial quality because of their advanced technology, fewer units, and much less accumulated operational time. Space life support systems have even more difficulty achieving high quality due to often building only single units and having limited ability to test and redesign. Quality that seems reasonable based on everyday experience is not easily achieved for military and space systems.

When new high technology systems are developed, there are always design errors, unexpected failures, and R&M problems. Newly designed systems "will invariably have reliability and performance deficiencies that generally could not be foreseen and eliminated in early design stages." (DOD Guide, 2005, 4-33)

The usual approach to high technology development makes these problems worse. The main focus of design is usually on meeting difficult performance requirements rather than easing long term operations. Sustained performance depends on designing for R&M and requires a long operating period to confirm. Designers often prefer to use advanced technology or improve performance requirements or add new features. Advanced technology, better performance, and additional features all increase the chance of design errors and operational failures and tend to reduce R&M performance.

The difficulty and uncertainty of the design process tends to reduce the time available for integration and test, which is needed to discover any problems that require redesign and retest. Time pressure increases the chance that a delivered system will have undiscovered problems that will appear during operations.

B. R&M for different missions

A Mars mission clearly has much higher risk than ISS or a moon base. The duration of operations independent of Earth is the major variable. In the Earth-moon system, the independent operation time is the return flight time of 2 or 3 days. A Mars round trip with a long surface stay requires about 900 days of independent operation time. A Mars mission life support system should probably have multiple units, not a single protoflight system, and more extensive R&M design and testing than ISS or a moon base. It may be useful to develop a higher R&M Mars-capable life support system for a moon base, before it is actually needed.

C. An assumptions-based or systems analysis approach to designing future life support?

The NASA R&M standard assumes that the usual well known systems engineering approach will be used. The mission and crew R&M needs should be assessed, requirements defined, alternatives developed, and trade-offs conducted to select a suitable R&M approach. The R&M development should be integrated with the rest of the system engineering development process, so that overall performance and costs can be optimized to meet all the system requirements. The systems development process begins with top level needs and works down to detailed modeling, designing, development, and testing. R&M is difficult to improve for an already existing design. The NASA standard indicates that obtaining satisfactory R&M requires designing it in from the beginning as part of the overall system design.

Life support has accomplished much in detailed engineering, especially working toward completing closure and improving the International Space Station (ISS) life support system, but it has not done a full top-down systems engineering analysis for future moon or Mars mission needs. Life support for more than fifty years has assumed that all future long duration human missions will use regenerative life support. This was justified by the very high cost of launching mass that prevented simply providing water and oxygen as is done for short missions. Now the cost of launch has been greatly reduced and the necessity of high closure recycling life support should be reconsidered. This is especially important for the cases such as oxygen generation where the current ISS recycling system has more mass than the oxygen it would supply during a Mars round trip. Although resupply has much higher mass than recycling for long missions, it has much higher reliability and much lower development cost. The overall best system, considering overall performance and cost including R&M may be a hybrid resupply/recycling system.

It has been generally assumed that future regenerative life support will have the traditional systems architecture implemented in the ISS and will use refined subsystems similar to those on ISS. This creates two problems for R&M. First, since the ISS life support operates in Low Earth Orbit (LEO) where resupply and crew return are more possible, it was not designed for the high level of R&M needed for deep space and Mars. And the R&M experienced on ISS has been poorer than originally expected. Achieving satisfactory R&M for deep space with ISS based systems will be difficult. Second, developing the optimum R&M may require an unconstrained clean sheet design

with system wide trade offs, such as suggested by the NASA R&M standard. This may produce a system design that differs significantly from the traditional systems architecture and subsystem implementations on ISS.

The ISS life support community assumes that future long duration life support will be similar to that on ISS, but the NASA systems engineering approach requires an unconstrained requirements based analysis and design. This situation seems to require considering both design options, a refined ISS life support system with improved R&M and an optimized clean sheet design. The R&M requirements will be an important factor, but they vary with mission location and distance. While a Mars mission requires much better R&M that ISS, a moon mission could operate with R&M performance similar to ISS. It would be helpful if a moon base life support had the better R&M required for Mars, but the Constellation moon project correctly did not consider it necessary.

D. Incremental improvement or new design approach?

There are two fundamental approaches to developing new hardware with better R&M and other performance, incremental improvement or new design. By far the most common engineering approach is a cautious redesign. Totally new designs are risky and rare.

However, the new NASA R&M guide is intended to guide the top-down development of a new system. It and other NASA directions remind us to use the standard phased project process, considering the customer, requirements, alternates, and trade-offs as prescribed by systems engineering procedures.

Like most engineering development programs, life support research is not simply developing an all new system following the traditional top-down systems engineering approach. Life support has conflicting visions, including achieving high closure, refining the ISS life support system, or developing advanced technologies. All of these advance life support but also somewhat differ from developing the most cost-effective design for a specific future long duration mission, which would be a reasonable goal for a top-down systems engineering approach.

There is an essential difference between staying as close as possible to tested systems and doing something new for the sake of innovation. How much freedom or motivation should the designers have to make changes? Even starting based on a regenerative system similar to space station life support, any of the functional subsystems could be refined, significantly redesigned, or even replaced by open loop resupply to improve R&M.

To improve R&M, the first step after defining the R&M requirements would be to assess how they can be achieved. Is refining the ISS technologies sufficient or is more extensive redesign needed? This determination may differ for each functional subsystem. The degree that the R&M requirements can be achieved will also depend on trade-offs with other requirements, engineering constraints, and overall management priorities. Since it is a future operations problem, R&M may receive insufficient priority and resources during development.

E. Closed or open loop life support?

The two traditional life support design architectures are resupply of oxygen, water, and lithium hydroxide to remove carbon dioxide, and regenerative recycling as used on the ISS. It was long assumed that the high cost of launch would make regenerative systems absolutely necessary for long duration missions. Any costs, difficulties, and operational needs of recycling would have to be solved or accepted. The new low launch costs now suggest that resupply will be better than recycling for much longer missions. If the mission planners focus on cost and the astronauts on reliability, they may prefer resupply.

Life support is more a functional category than an integrated system. Many of its functions are substantially isolated from the others or interface only through the habitat atmosphere. Even major systems, such as carbon dioxide removal, water recycling, and oxygen recycling, can be designed, tested, launched, and operated independently. The different technologies used in life support may have different R&M requirements and approaches.

The diminishing returns of increasing closure and the gradual implementation of life support life support on ISS suggest that the replacement of resupply by recycling for longer missions can be made step by step, with the highest payoff systems implemented earlier in the mission. The best system for a given mission may be a hybrid system with intermediate closure. Life support R&M should be understood for both resupply and recycling. R&M for storage containers and tanks is simple, but R&M of complex equipment is a major concern.

F. How can we obtain satisfactory R&M in NASA life support?

R&M can be improved by cutting performance requirements, avoiding new and complex technology, and allowing sufficient time for testing and redesign, but much more analysis and planning is needed. There is no known procedure that guarantees satisfactory R&M and, as mentioned, the NASA R&M standard and requirements are not defined prescriptions of an R&M process, but must be tailored to the specific system under development.

The first direct step in R&M for a new design is to establish the overall R&M approach and plan. The new and innovative approach of the R&M standard NASA-STD-8729.1A works top-down in stages and is intended to be applied at the project's beginning. This up-front design for R&M seems more likely to succeed that the previous approach of performing specific analysis throughout system development cycle.

The most important R&M decision is developing the R&M concept, which includes determining the level of repair and defining the maintenance method. On ISS the key R&M approach is to replace major subsystems as needed using on-board spares. The subsystems have Orbital Replacement Units (ORUs), which tend to be large with each one able to repair only a single failure. It is often suggested that lower level part repair would require more but smaller spares, saving launch mass but requiring more crew time, facilities, tools, and training. The new lower launch cost now makes the use of the larger ORUs more feasible. This solves one of the major problems with using the ISS life support as a model for future systems. It may well be worth providing the mass of ORUs to improve R&M and reduce crew time. The new lower launch costs make reducing launch mass much less important, so the optimum solutions would tend to have higher mass than in the shuttle era.

All R&M risks should be well analyzed and quantified, relying more on historical data than theoretical best cases. Safety risks especially must be considered. We have nearly ten year's experience with the ISS life support system, including failure reports and analysis. There are extensive plans for redesign to remove ISS life support failure modes. Improving reliability is greatly helped by reporting and analyzing all problems, failures, and off-nominal behaviors. A failure reporting process should be established at the beginning of new life support design.

To develop future life support systems with high safety and good reliability and maintainability, the systems must be carefully designed with any necessary sacrifices in performance and costs. Multiple units must be developed and tested over long periods, comparable to the mission duration, to adequately assess the failure rates and number of spares needed. All failures must be recorded, analyzed, traced to their root causes, and the failure causes designed out of the system. Eliminating all risk is not possible, so it is important to understand how much risk is being accepted. Using resupply rather than recycling or a mission to the moon rather than Mars would make providing safe and reliable life support much easier. It seems that the initial exploratory design studies should be unconstrained, and that their cost and risk optimization results should define the approach to take, including incremental or new, open or closed life support.

A space life support system is a loosely integrated system with very different subsystem functions and technologies. Even if the R&M requirements are similar for all subsystems, as they probably should be, the R&M design approach and implementation may differ between subsystems.

G. Would life support be developed in-house or under contract?

Will the future life support system be designed in-house by NASA, under contract, or differently for different subsystems? The earlier NASA R&M standard and the DOD Guide assume that a large well defined hardware and software system will be procured under an industry contract. This could well be true for a future NASA life support flight system. In this case, defining the R&M requirements and their verification takes precedence over providing NASA technical guidance in achieving the required R&M. Imposing specific R&M design methods could be regarded as over constraining and improperly guiding the contract, reducing the developer's flexibility and responsibility.

Even if the flight hardware is developed under contract, there is an important R&M role for NASA life support. Well before the R&M requirements are defined for the next mission, the life support research program must investigate and understand how to design for R&M. Life support has some subsystems that are independent or loosely coupled and could be developed independently. Some may be Government Furnished Equipment (GFE) supplied to the system integrator, built either under different contracts or by NASA directly. Most important, life support research must include R&M considerations in technology selection and subsystem development.

H. Could we use automation or computer based tools?

The current ISS life support architecture with similar subsystems was first tested with humans in a closed chamber in 1966. Since then the work place, the automobile, and the globe have been computerized and connected. A car now has dozens of networks and computers. The ISS life support system was originally required to have automated Fault Detection Isolation and Recovery (FDIR), but it was found difficult and impractical to implement. Building in automated R&M features would be a significant undertaking, and automation, like R&M, would need to be included in the initial design. Computer based test procedures, diagnostics, and maintenance instructions would be helpful and much easier to use.

I. Initial approach to achieving improved R&M in life support

It seems necessary to establish an overall R&M approach and plan before beginning work, but the above high level issues impact the implementation of R&M and changed decisions concerning them would affect the R&M plan. The best initial approach may be to identify a life support subsystem now under investigation and performing some important function that is relatively independent of the others and begin to analyze and design it to meet the R&M and other requirements. The carbon dioxide removal system seems a good candidate. Perhaps one heritage and one all new design could be investigated, or a preliminary trade off study could be done.

V. Conclusion

Achieving satisfactory reliability and maintainability in space life support will be difficult. Improving an existing system requires making incremental changes which require increasing effort and produce diminishing returns. For an existing system, the appropriate reliability and maintainability may be what can be achieved with the available resources rather than what was initially expected. The alternative of developing a new clean sheet design to meet difficult reliability and maintainability requirements would probably force designers to reduce other performance measures and use conservative technical approaches.

A system's reliability and maintainability can be planned, designed for, and predicted, but its actual performance can be very different from expectation. There are usually two stories about reliability and maintainability, one during development and a different one after operations. The story during development explains how the proper engineering design steps are being taken and how performance is expected to be satisfactory. The story after operational experience is often about why performance was not satisfactory due to unavoidable engineering limitations or external constraints. The ISS life support used new relatively untested pumps to save mass and had little integrated testing because of lack of funds. Some measures of reliability and maintainability have been much less than was predicted, but this seems inevitable in most projects.

A future life support reliability and maintainability engineering effort will be very successful if we can tell the same story after operations that we told during development and delivery. This requires that risks be correctly assessed, mitigated to the extent feasible or practical, and accepted where necessary. The system reliability and maintainability should be realistically, not optimistically predicted.

References

Carlson, C., Sarakakis, G., Groebel, D. J., Mettas, A., "Best Practices for Effective Reliability Program Plans," Reliability and Maintainability Symposium (RAMS) Proceedings, Jan. 28, 2010, www.reliasoft.com/.../2010_RAMS_best_practices_for_effective_reliability_program...., retrieved 11/20/2017.

DOD Guide for Achieving Reliability, and Maintainability (RAM), August 3, 2005.

Feather, M. S., Evans, J., and Cornford, S. L., "Identifying Where Mission Assurance Can Benefit from Model Based Systems Engineering," AIAA 2016-5543, AIAA SPACE 2016, 13 - 16 September 2016, Long Beach, California.

Jones, H. W., "Axiomatic Design of Space Life Support Systems," ICES-2017-82, 47th International Conference on Environmental Systems, 16-20 July 2017, Charleston, South Carolina.

NASA-STD-8729.1, Planning, Developing, and Managing an Effective Reliability and Maintainability Program, 12, 1998.

NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems, 6/13/2017.

NPD 7120.4E, Program/Project Management Policy, 6/26/2017.

NPD 8700.1E, NASA Policy for Safety and Mission Success, 12/6/2013

NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy, 4/18/2008, 4/16/2013.

NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, 8/14/2012.

NPR 7123.1B, NASA Systems Engineering Processes and Requirements, 4/18/2013.

NPR 8705.2C, Human-Rating Requirements for Space Systems, 7/10/2017.

NPR 8705.5A, Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, 6/7/2010.