The New NASA Approach to Reliability and Maintainability

Harry W. Jones, Ph.D., MBA, NASA Ames Research Center

Key Words: reliability, maintainability

SUMMARY & CONCLUSIONS

In 2017, after 20 years, NASA issued a major revision of its reliability and maintainability (R&M) policy, NASA-STD-8729.1A [1]. Formerly NASA required certain specific R&M activities during each succeeding phase of project development. Now NASA requires a project to start by including the initial development of R&M requirements and the devising of strategies to implement and verify them. Rather than resolving 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. It begins by first identifying the top level requirements and suggesting top level design strategies for those, then making these higher strategies the basis for a lower level set 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 later with difficulty to a completed design concept. The new R&M standard uses an innovative and effective top-down system design approach intended to effectively implement R&M.

1 INTRODUCTION

The new 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 the implementation of 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. 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.

2 NASA RELIABILITY AND MAINTAINABILITY DOCUMENTS

The three most important NASA R&M documents are shown in Table 1.

Table 1 – NASA R&M Documents

Number	Title
NASA-STD-8729.1A	NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems [1]
NPD 8720.1C	NASA Reliability and Maintainability (R&M) Program Policy [2]
NPG 7120.5E	NASA Space Flight Program and Project Management Requirements [3]

NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems, is the key NASA R&M document, issued in 2017 [1]. The previous version was issued in 1998 and was very different. NASA-STD-8729.1A's governing document is NPG 7120.5E, NASA Space Flight Program and Project Management Requirements [3]. The applicable policy directive is NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy [2].

2.1 *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 [2] 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-8729.1A.

2.2 *NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems [1]*

The purpose of NASA-STD-8729.1A 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." [1, 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." [1, p. 3]

As always, the R&M requirements must be verified, by either 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 and strategies are respectively the R&M requirements and the hardware designs or other activities developed to satisfy 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.

The standard includes the broad technical objectives and strategies that affect 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." [1, p. 5]

3 IMPLEMENTING THE NEW NASA RELIABILITY AND MAINTAINABILITY (R&M) STANDARD

This section includes R&M objectives and strategies, evidentiary methods, and requirements planning and implementation.

3.1 *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 [4].

3.2 *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.

3.3 *R&M requirements planning and implementation*

8729.1A [1] states that the R&M requirements should be planned and implemented in the Safety and Mission Assurance (SMA) plan required by NPR 7120.5 [3]. 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:

- R&M criteria, including those derived from safety, logistics, etc.;
- R&M functional requirements and performance objectives that support R&M activities such as quantitative reliability models and Failure Modes and Effects Analysis (FMEA);
- Design and process standards impacting system reliability;
- The R&M products used as evidence that the strategies that were implemented and objectives achieved, considering the suggested evidentiary methods in 8729.1A;

- Any R&M products used for design requirement verification;
- The strategy for independent evaluation of R&M products and activities.

4 THE PREVIOUS NASA RELIABILITY AND MAINTAINABILITY (R&M) STANDARD [5]

The earlier NASA R&M standard was published in 1998 and 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 earlier standard provides generic guidance and unlike the new revision was not mandatory. The earlier was for use on all new and existing NASA programs, while the revision is for new programs only.

This previous standard emphasized R&M integration with other organizational elements, including Quality Assurance, Human Engineering, Logistics Support, and Project Engineering. It also emphasized R&M as part of the system acquisition process, with specific activities defined for R&M during program 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 earlier and the revised R&M standard is to implement a requirements based, not process based procurement. The 1998 Goldin era earlier standard observed, "(T)he new process of holding contractors accountable for their final product transfers much of the cost, risk, and quality responsibility from NASA to the contractor." [5, p. 4-3] The R&M performance requirements are part of the system end item performance specification. [5, p. 8-2]

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

- Definition of operating environment,
- Definition of system failure,
- The minimum R&M performance requirements, and,
- 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." [5, p. 8-2]

R&M engineering should perform the appropriate R&M trade-off studies including:

- reliability prediction
- R&M allocation
- failure modes and effects analysis
- criticality analyses
- fault tree analysis
- worst case circuit analysis
- maintainability assessment [5, 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:

- accessibility
- interchangeability
- failure detection
- failure isolation
- special tools and diagnostics
- spares
- logistics support sources [5, p. 8-5]

The essential difference between 8729.1 [5] and the revised 8729.1A [1] is that the earlier aimed more directly at defining 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 the revision expand the similar R&M toolsets utilized in the previous standard.

5 THE R&M OBJECTIVES AND STRATEGIES FROM NASA-STD-8729.1A [1]

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.

5.1 *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.

5.2 *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 "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.

5.3 *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 "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 straightforward project flow is not reflected in the new objectives based approach.

5.4 *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 affecting 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.

5.5 *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 checkout.
            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 Reliability Centered Maintenance (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.

6 DISCUSSION

The revised NASA Reliability and Maintainability (R&M) Standard, NASA-STD-8729.1A, NASA Reliability and Maintainability Standard for Spaceflight and Support Systems, [1] was updated to conform to the objectives-based management approach of NPR 7120.5E, NASA Space Flight Program and Project Management Requirements [3]. The revision was developed by an experienced team of NASA R&M engineers to provide a modern and comprehensive view of R&M linked to top-level objectives. Using objectives in a hierarchy improves systems engineering and risk management. "The revised standard is an innovation for Safety and Mission Assurance disciplines and leads the way in advancing the vision of objectives-based standards."[4] "The implementation of this revised standard will promote technical excellence in the field and will enable innovations as well." [4]

REFERENCES

1. NASA-STD-8729.1A, NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems, 6/13/2017.
2. NPD 8720.1C, NASA Reliability and Maintainability (R&M) Program Policy, 4/18/2008, 4/16/2013.
3. NPR 7120.5E, NASA Space Flight Program and Project Management Requirements, 8/14/2012.
4. M. S. Feather, J. Evans, S. L. Cornford, "Identifying Where Mission Assurance Can Benefit from Model Based Systems Engineering," AIAA 2016-5543, AIAA SPACE 2016, 13 - 16 September 2016, Long Beach, California.
5. NASA-STD-8729.1, Planning, Developing, and Managing an Effective Reliability and Maintainability Program, 12, 1998.

BIOGRAPHY

Harry W. Jones, Ph.D., MBA
N239-8
NASA Ames Research Center
Moffett Field, CA 94035, USA

e-mail: harry.jones@nasa.gov

Harry Jones is a NASA systems engineer working in life support. He previously worked on missiles, satellites, Apollo, digital video communications, the Search for Extra Terrestrial Intelligence (SETI), and the International Space Station (ISS).