The New NASA Approach to Reliability and Maintainability

Harry W. Jones, Ph.D., MBA

Overview

- The recent NASA technical standard on R&M has moved away from requiring specific R&M activities during each of the traditional project phases.
- Now NASA will plan and design to meet R&M requirements that satisfy the project R&M objectives.
  - The top level R&M objective is defined.
  - Design strategies to implement it are developed immediately.
  - Then the next lower objectives are defined and strategies designed.
  - This step-by-step, top-down approach is similar to axiomatic design.
- The new R&M process is aligned with the systems design process and helps ensure that the methods needed to meet the R&M requirements are built into the design.

New NASA R&M Standard

- In 2017 after 20 years, NASA revised its R&M standard.
  - Before NASA required specific R&M activities during each phase of project development.
- Now NASA requires a project to start by developing the R&M requirements and strategies to implement them.
  - And rather than doing all the requirements first and then designing the system, as usual in systems design, the design process now is to work top down by layers.
- This approach is intended to ensure that R&M is designed in from the beginning rather than added with difficulty to an already completed design concept.

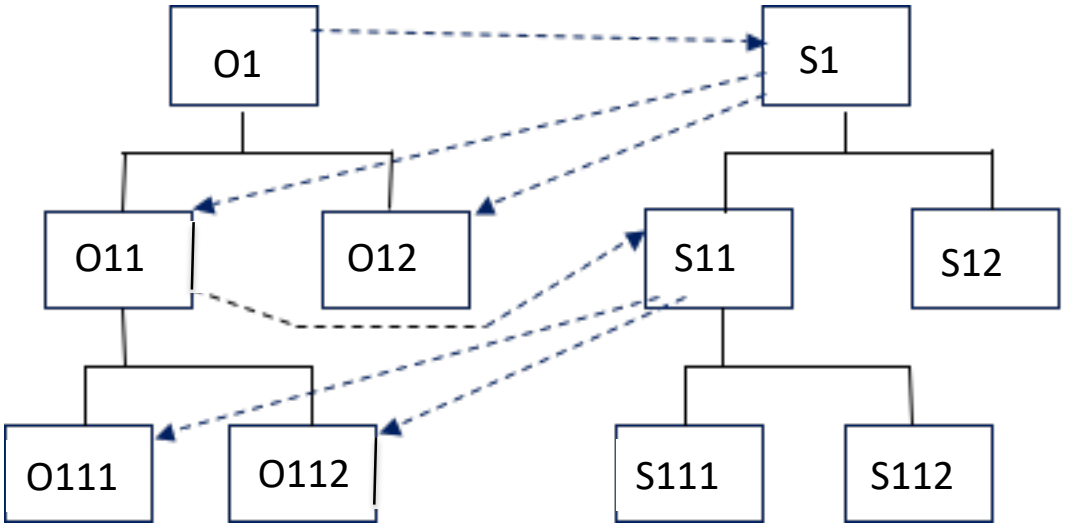
NASA R&M policy

- R&M policy requires a program to define its maintenance concepts, requirements, activities, and schedule.
- R&M design assumes the full system engineering design and development process will be carried out and that R&M will be integrated into it.
- R&M must be coordinated with risk management, safety, security, quality assurance, logistics, probabilistic risk assessment, life-cycle cost, and configuration management.

More on the R&M Standard

- NASA now plans to develop and implement tailored R&M requirements to meet the top level project R&M objectives.
  - The emphasis is on proving the R&M requirements will be met.
  - The new standard applies only to new NASA projects, since it is intended “to assure reliability is designed and built into systems.”
- The new approach defines a comprehensive hierarchy of R&M objectives and identifies specific strategies to implement them at each level.
  - The objectives are the R&M requirements, and the strategies are designs or plans developed to meet the requirements.

Mapping objectives to strategies



- Objectives and strategies are developed by -
  - Defining an objective in the functional domain.
  - Creating a strategy in the strategies domain.
  - Defining subobjectives to implement that strategy.
  - And so on.

The R&M planning process

- The R&M standard has14 objectives and 49 strategies.
- The R&M strategies must be verified.
  - The 49 strategies are each provided with suggested evidentiary methods, such as testing, failure analysis, derating, and many others.
  - There are 69 R&M evidentiary methods, including reliability and maintainability analysis, test, and evaluation.
  - Not all evidentiary methods are required.
  - Others can be used.
- R&M planning should include R&M products that show the strategies were implemented and objectives met.

The R&M top objectives

- Top objective: system performs as required over the lifetime to satisfy mission requirements.
- The top objective has four subobjectives;
  - Subobjective 1: The system conforms to the design intent and performs as planned.
  - Subobjective 2: The system remains functional for the intended lifetime, environment, operating conditions, and usage.
  - Subobjective 3: The system is tolerant to faults, failures, and other anomalous internal and external events.
  - Subobjective 4: The system is designed to accommodate an acceptable level of availability and maintenance demands.

Subobjective 1- design, test, and early fault correction

- 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.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.2 Objective: All issues resolved or closed out to an acceptable level of risk.
  - 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.

Subobjective 2 - eliminate failures, estimate reliability

- 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.2 Objective: System or its elements are not susceptible to common cause failures.
  - 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.

Subobjective 3 - fault tolerance

- 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.2 Objective: Physical and functional pathways for fault propagation are limited.
    - 3.A.3 Objective: System is able to recover from anomalies affecting functions that are important to top-level expectations.
    - 3.A. 4 Objective: System can degrade or lose functions without significantly impacting top-level expectations (through contingency operations).

Subobjective 4 - acceptable maintainability

- Subobjective 4: The system has an acceptable level of maintainability and operational availability.
  - 4.A.1Strategy: Evaluate, control, and monitor the ease of maintaining, restoring, or changing system capability and total maintenance demands.
    - Objective: Maintenance and repair activity can be performed within available resources (cost, time).
    - Objective: System provides clear indication of health status, degradations, and diagnostic information.
    - Objective: System design allows for reconfiguration, upgrade, or growth opportunities during the mission.
    - Objective: Maintainability performance is validated and optimized during operation based on available maintenance data.

Evidentiary methods

- The R&M standard has 69 evidentiary methods to verify the 49 strategies.
- Reliability Analysis
  - Approved Parts and Parts Traceability
  - Failure Mode and Effects Analysis (FMEA)
  - Fault Tree Analysis (FTA)
  - Reliability Modeling
- Reliability Testing
  - Acoustics, Shock, Thermal, and Vibration Tests
  - Electromagnetic Compatibility Test
  - Life Test
- Maintainability Methods
  - Logistics and Maintenance Plan
  - Maintainability Demonstration
  - Problem Failure Reporting
  - Reliability Centered Maintenance

Developing the R&M plan

- The three steps to develop an R&M plan:
  - 1. Establish the reliability and maintainability vision and approach.
  - 2. Select the most applicable of the dozens of reliability methods and strategies.
  - 3. Identify potential problems that may block achieving the R&M vision, such as,
    - Lack of test time.
    - Lack of management support.
    - Lack of understanding of reliability.
    - Lack of learning from failure.

Conclusion - R&M approach

- Focus on the few key reliability and maintainability methods that are needed to achieve the objectives.
- Emphasize the tasks that achieve reliability as early as possible.
- Emphasize methods to improve rather than analyze reliability.
- Safety first, separate from and more important than R&M.
- Success requires sufficient management support, resources, reviews, and active problem solving.