Recommended Reliability, Availability and Maintainability Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications
Revised 2025 (7 Pages)

A.   Purpose

This Manual Part recommends Reliability, Availability and Maintainability (RAM) assurance programs for electronic/software-based products used in vital signal applications.

B.   General

1.   The reliability, availability and maintainability of electronic/software-based products are fundamental design requirements that should be considered as a part of an integrated approach to system assurance. Reliability, availability and maintainability are separate issues and have distinctly different requirements but the programs for achieving these requirements are similar.

2.   The objective of the reliability assurance program is to provide assurance that the product meets its specified reliability requirements.

3.   The objective of the maintainability assurance program is to provide assurance that the product meets its specified maintainability requirements.

4.   The objective of the availability assurance program is to provide assurance that the product meets its specified availability requirements.

5.   An integrated program for the management of Quality, Reliability, Availability and Maintainability should be in place, consisting of:

    a.   A Quality System conforming to Manual Part 17.2.1 Recommended Quality Assurance Program for Electronic/Software Based Products Used in Vital Signal Applications.

    b.   Reliability, availability and maintainability assurance programs consisting of the following elements:

        (1)   Program Plan;

        (2)   Requirements;

        (3)   Requirements Allocation;

        (4)   Detailed Analyses;

        (5)   Verification & Validation;

(6)   Re-verification/Re-validation of Modifications; and

(7)   Failure Reporting.

6.   The system, subsystem and product boundaries and functions should be clearly defined and documented in order to clearly identify and assess the impact on RAM requirements.

7.   The programs described in this Manual Part should be considered guidelines. The actual reliability, availability and maintainability programs should be tailored to the requirements of the manufacturer, user and the product involved.

C.   Reliability, Availability and Maintainability Management

1.   Reliability, Availability and Maintainability Program Plan

a.   The RAM Program Plan provides a structured approach to planning and implementing the overall Reliability, Availability and Maintainability assurance program. It should identify the RAM assurance activities and RAM-related documentation for the product under development.

b.   RAM reviews should be planned and conducted during the product development phases to ensure that RAM assurance activities are carried out at their appropriate times, and reliability issues are resolved in a timely manner.

D.   Reliability Management

1.   Reliability Requirements

a.   The reliability requirements may be stated in terms of an overall product failure rate (failures per unit time), a Mean Time Between Failures (MTBF) and should be developed alongside the availability requirements.

b.   Reliability requirements should be based on the functional requirements, user requirements, and general reliability concerns over the lifecycle of the product under consideration.

c.   Consideration shall be given to the most severe class of operating environment in which the product is intended to operate. See Manual Part 11.5.1 Recommended Environmental Requirements for Electrical and Electronic Railroad Signal System Equipment and Manual Part 11.5.2 Recommended Electromagnetic Compatibility Immunity and Emissions Testing for Signaling Products.

2. Reliability Requirements Allocation

   a. The reliability requirements should be allocated to the hardware and software subsystems based upon the nature of the requirements and architectural design of the product. Where required, the allocation of each reliability requirement should be documented with respect to how it relates to any higher-level reliability requirements specified by the user.

3. Detailed Reliability Analyses

   a. These analyses should provide detailed hardware failure/fault rate predictions using established techniques, such as Failure Modes, Effects, and Criticality Analysis (FMECA), Reliability Block Diagrams (RBD) and historical data, to ensure compliance with the reliability requirements and allocations.

   b. The fault rate of each key building block (such as printed circuit assemblies) of an electronic/software-based product should be kept as low as possible by proper component selection, de-rating, and application. Fault rates should be predicted during the design phase using prediction analysis methods (e.g., U.S. MIL-HDBK-217F(2) Parts Stress Method, IEC 62380) or historical data.

   c. The predicted rates should be used as a check on proper component selection, de-rating, and application in the specified environment. Consideration should be given to historical data and to mitigating traditionally unreliable components such as connectors and plug-in sockets.

   d. Software reliability should be assured through a quality assurance Program conforming to Manual Part 17.2.1 Recommended Quality Assurance Program for Electronic and/or Software Based Products Used in Vital Signal Applications, and a rigorous verification and validation program.

4. Reliability Verification & Validation

   a. The Reliability Verification & Validation should demonstrate compliance of the product with all reliability requirements. The final design should be reviewed and documented to confirm that the product meets its reliability requirements. In-service data over a sufficient period of time should be used to assess the reliability of the product.

   b. For new products, use of predictive analyses (with correction factors where applicable) should be used to understand the ability of the

design to meet the reliability requirements prior to product release and until sufficient in-service data is available.

5.   Re-verification/Re-validation of Modifications

a.   Hardware, software and application-related modifications made subsequent to release of the product should be verified and validated to demonstrate that the modified product is still compliant with the requirements.

6.   Failure Reporting

a.   A failure reporting system should be in place to record and track the resolution of the hardware/software faults and product failures during the development, production and service lifecycle phases of the product.

E.   <u>Maintainability Management</u>

1.   Maintainability Requirements

a.   The objective of this step is to identify the overall maintainability requirements of the product, based on the overall functional requirements, user requirements, and maintainability concerns over the lifecycle of electronic/software-based products in general. The requirements may be stated in terms of an Individual Line Replaceable Unit Mean Time to Replace (IMTTR), Overall product Mean Time to Restore (OMTTR), and as a part of a product availability requirement.

b.   Consideration should be given in the design to system modularity and to self-diagnostic facilities.

c.   Consideration should be given in the design of the product to have the ability to transmit the results of the self-diagnostic tests to a remote facility.

d.   Consideration should be given in the design to simplifying the fault identification, operational and functional testing requirements of the product so that the OMTTR of the system is minimized.

e.   The IMTTR should be considered as a subset of the OMTTR and shall exclude the major architectural structural items of the product (motherboard, chassis, etc.), travel time, initial fault analysis, spare product availability, employee experience etc., and be directed specifically at module design and replacement requirements of essential modules and I/O devices, based on site diagnostic results and related functional testing. The IMTTR time considered in the

design should be no longer than 30 minutes per affected module/fault.

2. Maintainability Requirements Allocation

    a. The Maintainability Development program should include a Maintainability Requirements Allocation phase to establish and document the maintainability requirements of the product. The objective of this step is to allocate the maintainability requirements to both hardware and software portions based upon the nature of the requirements and architectural design.

    b. Where required, the allocation of each maintainability requirement should be documented with respect to how it relates to any higher-level maintainability requirements specified by the user.

3. Detailed Maintainability Analyses

    a. Detailed maintainability analyses consisting of review of the hardware and software maintainability features being built into the equipment/system (modular design, built-in test features, mechanical packaging, etc.) should be conducted on the equipment/system as the design progresses. The objective of these analyses is to ensure compliance with the Maintainability Requirements Allocation.

4. Maintainability Verification & Validation

    a. The objective of this step is to demonstrate compliance with all maintainability requirements. The final design should be reviewed and documented to confirm that the product meets its maintainability requirements. A maintainability demonstration using simulated faults in hardware/software, with the product configured in its final application environment should be conducted to assess the maintainability of the product.

5. Re-verification/Re-validation of Modifications

    a. Hardware, software and application-related modifications made subsequent to release of the product should be verified and validated to demonstrate that the modified product is still compliant with the requirements.

6. Failure Reporting

    a. A failure reporting system should be established to record and track the resolution of the maintainability issues during the development, production and service lifecycle phases of the product.

F. Availability Management

1. Availability Requirements

    a. The availability requirements should be stated in terms of a percentage (or probability) that reflects the ability of the product to be in a state to perform its required function under given conditions at a given instant of time.

    b. Availability is determined as a combination of the reliability and maintainability parameters based on the following:

    $$Availability\ (\%) = \frac{Mean\ Uptime}{Mean\ Uptime + Mean\ Downtime} = \frac{MTBF}{MTBF + MTTR}$$

    c. Availability requirements should be based on the functional requirements, user requirements, and general availability concerns over the lifecycle of the product under consideration.

2. Availability Requirements Allocation

    a. The availability requirements should be allocated to the hardware and software subsystems based upon the nature of the requirements and architectural design of the product. The hardware and software of the product may have to be designed with the ability to be configured in active or standby modes to meet product availability requirements.

    b. Where required, the allocation of each availability requirement should be documented with respect to how it relates to any higher-level availability requirements specified by the user.

3. Detailed Availability Analysis

    a. The Availability analysis should be based on the product MTBF and MTTR values calculated in the Reliability and Maintainability analyses.

4. Availability Verification & Validation

    a. The Availability Verification & Validation should demonstrate compliance of the product with all availability requirements. The final design should be reviewed and documented to confirm that the product meets its availability requirements. In-service data over a sufficient period of time should be used to assess the availability of the product.

  b. For new products, use of predictive analyses (with correction factors where applicable) should be used to understand the ability of the design to meet the availability requirements prior to product release and until sufficient in-service data is available.

5. Re-verification/Re-validation of Modifications

  a. Hardware, software and application-related modifications made subsequent to release of the product should be verified and validated to demonstrate that the modified product is still compliant with the requirements.

6. Failure Reporting

  a. A failure reporting system should be in place to record and track the resolution of the hardware/software faults and product failures during the development, production and service lifecycle phases of the product.