Work Instruction

Reliability Prediction/Maintainability Assessment/Availability Analyses

Approved by:

_____

Gary G. Kelm., Chief
Program and Project Assurance Division

NASA - Glenn Research Center
Cleveland, OH 44135

Printed copies are uncontrolled and are not to be used for operational purposes.

Point of Contact: Jose A. Cruz/(216)433-3122

Change Record

Rev.	Effective Date	Description
Basic	Dec. 3, 1998	Initial Issue
A	Aug 27, 1999	CR007: Add quality records section; modify references, definitions, tools, training; update organizational names
B	May 17, 2004	CR068A: Revise 2.1, 6.5, 6.6 to include failure rate contribution of radiation; update organizational names
B	May 15, 2006	Document Review by P.O.C. no changes required - document updated to reflect organizational names plus new AFS numbering. Rev. change not required.
C	Aug 3, 2008	CR126: This revision adds interim reviews of analyses by members of an IPT that is defined as containing disciplines such as Systems Engineering, Risk Management, System Safety, and Probabilistic Risk Assessment (PRA). Confirm change of document number from GRC-W0510.061.
D	April 21, 2010	CR149: Replace Space Assurance Requirements and Guidelines (GLM-QE-8700.2) with Space Assurance Requirements (GLPR 7120.5.30), replace Program/Project/Subproject Office Assurance Team with Program and Project Assurance Division and Integrated Product Team in 2.1

1.0 PURPOSE

To define a process at Glenn Research Center to identify reliability, maintainability and availability parameters for flight projects at Glenn Research Center.

2.0 REFERENCES

Document Number	Document Title
NPR 7120.5	NASA Space Flight Program and Project Management Requirements
NPD 8700.1	NASA Policy for Safety and Mission Success
NPD 8720.1	NASA Reliability and Maintainability (R&M) Program Policy
NASA-STD-8729.1	Planning, Developing, and Managing an Effective Reliability and Maintainability Program
NASA SP-2007-6105	NASA Systems Engineering Handbook
GLPR 8700.4	Product Assurance
GLP-QE-8700.1	Roles, Responsibilities and Interrelationships of SMAD/SSQRD Support to GRC Programs/Projects
GLM-QE-8700.1	Product Assurance Manual (PAM)
GLPR 7120.5.30	Space Assurance Requirements (SAR)

2.1 Definitions and Acronyms

Destructive Event	A hard failure caused by radiation induced damage that requires a maintenance action.
IPT	Integrated Product Team: The Integrated Product Team is the team responsible for the Systems Engineering, hardware components design and selection, System Safety, Reliability and Maintainability, Probabilistic Risk Assessment, Risk Management, and Software Product Assurance (SPA) on the Program, Project, or Sub-project.
Maintenance Action	A removal, replacement, and testing of failed equipment or software.
Physical Zone	Regions of a circuit card or electronics box that are tested in a particular sequence. Testing various zones is usually performed due to the size of the test article as compared to the maximum radiation beam diameter available.
PPAD	Program and Project Assurance Division
P/P/S	Program/Project/Subproject
RAME	A Reliability, Availability, Maintainability Engineer designated by the Program and Project Assurance Division, and is a part of the Integrated Product Team.
Radiation Induced Failure Rate	The contribution to the total device failure rate due to the radiation environment of the intended mission.
Recoverable Event	A functional interrupt or data corruption that is detectable and can be cleared by re-initializing or re-booting a processor without a

	maintenance action.
SMAD	Safety and Mission Assurance Directorate
Trajectory Radiation Analysis	An analysis that determines at various points along the planned mission space trajectory, what the expected radiation environment should be. This analysis should provide parameters such as particle composition, energy level, total dose, and flux.

2.2 Quality Records and Forms

The Reliability Prediction, Maintainability Assessment, and Availability Analysis reports are the responsibility of the P/P/S and become part of the P/P/S Configuration Management System. However, analysis reports written by Program and Project Assurance Division (PPAD) will be archived in the PPAD office archive.

3.0 SAFETY PRECAUTIONS

Not Applicable

4.0 TOOLS, EQUIPMENT AND MATERIALS

Rapid Availability Prototyping for Testing Operational Readiness (RAPTOR) is a reliability block diagram program available from the U.S. Air Force.

5.0 PERSONNEL TRAINING AND/OR CERTIFICATION

NASA/TP 2000-207428 - Reliability Training
NASA Safety Training Center Course 0017 – Design for Reliability

6.0 INSTRUCTIONS – RELIABILITY PREDICTION

6.1 The P/P/S defines the system documentation. This documentation describes the design and operation of the system and may consist of the Baseline Concept Document, with functional block diagrams, a functional description, drawings, schematics, parts lists, materials, hardware map, specifications, and interface descriptions.

6.2 The P/P/S determines the component interfaces. Specifically, design engineering should provide a description of “connectivity” between subsystems, and between the system and its carrier vehicle or its facility. “Connectivity” implies paths along which energy or information may be transferred.

6.3 The P/P/S develops a description of how the system works. This should include: 1.) the definition of what constitutes successful system operation (mission success) 2.) the intended operating environment, 3.) stresses expected on major components during operation, 4.) required operating time for each major component, 5.) functional inputs and outputs for each major component.

6.4 The P/P/S engineers and RAMEs draw the reliability block diagrams. These diagrams should depict those components that must operate in series and in parallel (redundant configuration) in order to attain successful operation. If a Hazard Analysis has been or is in the process of being developed it can be reviewed at this point as an aid to determining

failure modes whose effects may impact safety. Even if a Hazard Analysis has not been developed design information and the reliability block diagram can be reviewed with system safety to assure mutual understanding of the system and its internal redundancy.

6.5 The RAMEs search for failure rate data or other statistical parameters consistent with the choice of failure distribution. Failure rate data may be selected from:

1.) actual experience data from very similar equipment in the same environment, 2.) experience data for similar equipment with a compensating factor for differences in environment, 3.) life test data, 4.) commercial, NASA, or military reliability databases, 5.) reliability handbook data, 6.) engineering judgement, 7.) expert elicitation

The failure rate contribution due to the radiation environment of the intended mission must be included as part of the total device failure rate for radiation susceptible devices. In order to achieve a meaningful estimate of the radiation induced part of the total failure rate, data from radiation testing that simulates the mission environment must be used. The radiation test data utilized must be based upon:

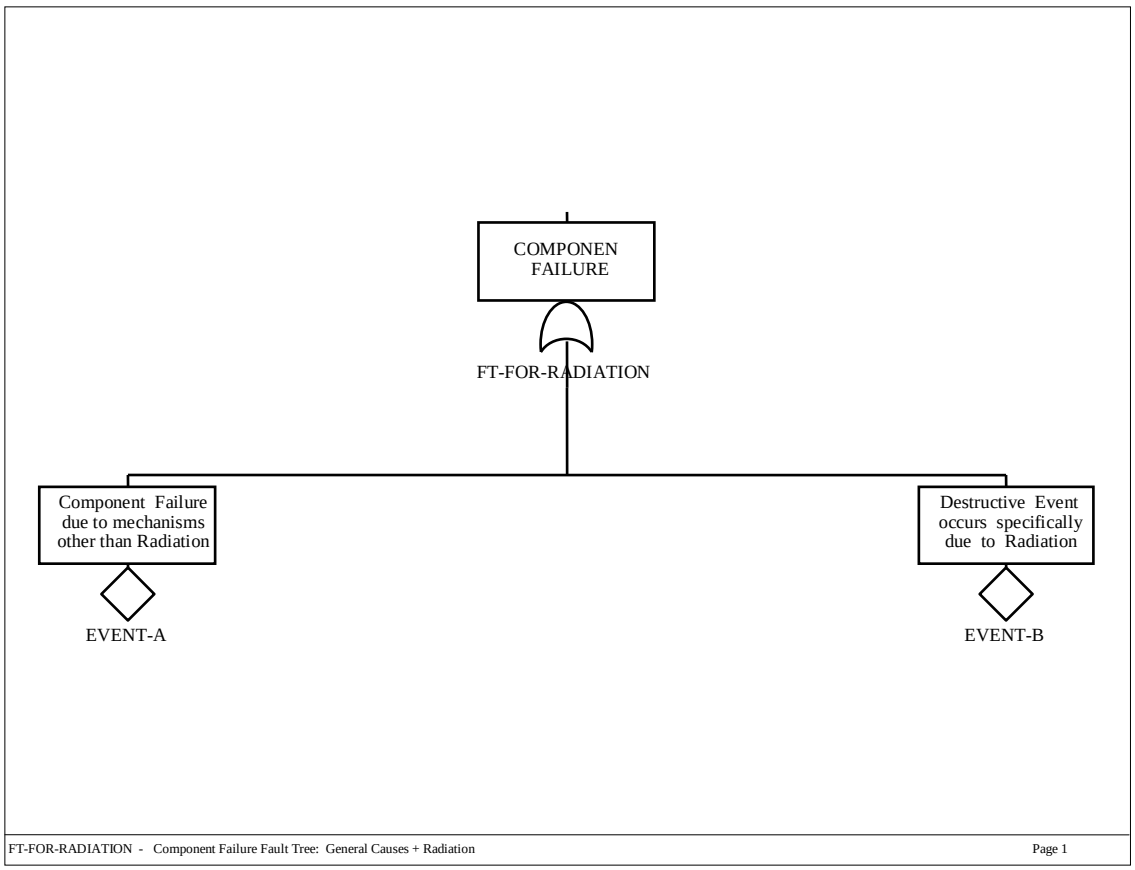
a.) Real-time monitoring of operational inputs and outputs during radiation exposure
b.) Destructive events detected on the circuit card or component
c.) All accumulated radiation (dose in kRad[Si]) and elapsed operating time (in seconds) up to the occurrence of the destructive event.
d.) Relevant radiation parameters: Fluence[#/cm^2], beam MeV, and average beam current [nA]
e.) Number of errors and error types
f.) The failure data for each physical zone of a circuit card or electronics box that is tested.

The radiation test plan and/or report must be reviewed to assure that the criteria (a) through (f) above are included. These criteria are necessary in order to show that the radiation test report can be used as a valid source of data for estimating the radiation induced failure rate. This is particularly important because the P/P/S must be able to understand the conditions under which failures occurred and to acquire the necessary input data to the radiation test evaluation program (computerized model) for calculating the failure rate. When the hardware under test sustains destructive events in different physical zones, the failure rates associated with these different zones must be combined (added) to find the worst-case radiation induced failure rate.

If the P/P/S requires that fault event rates should be determined for recoverable events, these rates shall be reported separately and should not be used as an input for the reliability analysis.

6.6 The RAMEs perform the reliability prediction for the design. Computations are performed to be consistent with the reliability model chosen.

When performing the calculations, the failure rate contribution due to the radiation environment must be included in the reliability model. At the component level, the following fault tree describes the two classes of failure events:



(1) $F(t) = F_a(t) + F_b(t) - F_a(t)F_b(t)$

$F(t)$ = The probability that the component fails at some elapsed mission time t.
$F_a(t)$ = The probability that the component fails due to failure mechanisms other than radiation at a mission time t.
$F_b(t)$ = The probability that the component sustains a destructive event specifically due to radiation at a mission time t.

The above equation leads to a equation for reliability that is the following:

(2) $R(t) = R_a(t)\, R_b(t)$.

$R(t)$ = The probability that the component <u>does not fail</u> at some elapsed mission time t.
$R_a(t)$ = The probability that the component <u>does not fail</u> due to failure mechanisms other than radiation at a mission time t.

$R_b(t)$ = The probability that the component <u>does not</u> sustain a destructive event due to radiation at a mission time t.

Based on NASA/TP 2000-207428, <u>Reliability Training</u> , Pg.42

(3) $R_a(t) = \{\exp[-\lambda_{operating}\, t_{operating}]\}\{\exp[-\lambda_{non\text{-}operating}\, t_{non\text{-}operating}]\}$

$$= R_{operating} R_{non\text{-}operating}$$

where $t_{operating}$ is the operating time of the device being analyzed, $t_{non\text{-}operating}$ is the non-operating time, $\lambda_{operating}$ is the failure rate which applies to the operating state that is due to failure mechanisms other than radiation, and $\lambda_{non\text{-}operating}$ is the contribution to failure rate from the non-operating state.

If d is the duty cycle of the device, then we have:

(3a) $t_{operating} = dt$

(3b) $t_{non\text{-}operating} = (1-d)\, t$

where t is the mission time. The above reliability function in (3) may be written as:

(4) $R_a(t) = \exp\left[-\{\lambda_{operating} dt + \lambda_{non\text{-}operating} (1-d)\, t \}\right]$

The radiation induced destructive events can be approximately described by an exponential failure distribution function and applies to the operating state.

(5) $R_b(t) = \exp\left[-\lambda_{radiation}\, dt \right]$

Where t is the mission time, d is the duty cycle, and $\lambda_{radiation}$ is the radiation induced part of the total failure rate. The complete formula for the reliability of the device is:

(6) $R(t) = \{\exp\left[-\{\lambda_{operating} dt + \lambda_{non\text{-}operating} (1-d)\, t \}\right]\} \times \exp\left[-\lambda_{radiation}\, dt \right]$.

Various types of earth orbits other than Low Earth Orbit, and trajectories for Deep Space missions (such as Mars, Jupiter, Saturn, and Neptune) may involve trajectories where the radiation environment changes as a function of spacecraft position on the trajectory. The motion of the spacecraft along its planned trajectory corresponds to a certain elapsed mission time t. In this case, the hazard rate, h(t) that describes the radiation induced destructive events may not be well approximated as a constant but will have to be obtained from a trajectory radiation analysis. The reliability equation for the component will change. In general,

(7) $R_b(t) = \exp\left[-\int_0^t h(\eta)_{radiation}\, d\eta \right]$.

6.7 The RAMEs compile the results of calculations and compare results to reliability design targets. Recommendations to improve the system reliability may be developed and/or components may be rank ordered by mean-time-between-failure (MTBF) [lowest (first) to highest (last)] with a recommendation on which components should be maintained and/or spared.

6.8 **IPT Review:** The preliminary reliability results are submitted for review by the **IPT.** This review enables the IPT to take the reliability analysis into account in the development of their designs and other analysis products. A result of this review may be changes to the analysis or a decision to perform trade studies. The RAMEs review the recommended additions, corrections, and deletions. These are discussed with originators. As a result of IPT review, additions, deletions, and corrections are made to the analysis.

6.9 Is a Trade Study needed? Results are discussed within the P/P/S. It may be decided to perform a trade study. In a trade study, various parameters are varied one at a time while all other parameters are held constant (as they were in the original reliability prediction analysis) in order to determine the impact on system reliability by the change in a specific parameter.

6.9.1 The P/P/S and RAMEs decide on trade-off parameters. Reliability improvement versus changes in system architecture, redundancy, sensors, components quality level, stresses, or intended operating time may be performed.

6.10 The RAMEs write a Preliminary Report.

6.11 The preliminary report is distributed to selected engineers for review. Engineers perform a technical review and note any needed corrections, or recommend deletions, and/or additions.

6.12 Is the analysis approved? YES: If the P/P/S agrees with the technical content of the report and its findings, the report may be simply revised. NO: If the report is disapproved, the RAMEs may return to step 6.4 and the entire process for the reliability prediction analysis may be reviewed. Errors in process will be corrected.

6.13 The RAMEs distribute the final (signed off) report and file.

7.0 INSTRUCTIONS – MAINTAINABILITY ASSESSMENT

7.1 The P/P/S defines the system documentation. This documentation describes the design and operation of the system and may consist of the Baseline Concept Document, with functional block diagrams, a functional description, drawings, schematics, parts lists, materials, hardware map, specifications, and interface descriptions.

7.2 The P/P/S writes the Maintainability Plan and the Maintenance Concept Document (MCD) for the system with the assistance of RAMEs. The Maintainability Plan details the specific maintainability engineering tasks that must be performed for the system design and operations planning. The MCD will describe the basic maintainability approach for the design.

7.3 An IPT reviews the MCD and the basic design from a systems perspective. The P/P/S should designate the preliminary line replaceable units (LRUs) or orbital replaceable units (ORUs).

7.4 The P/P/S performs a qualitative review of the design with RAMEs against maintenance criteria such as accessibility, alignment, removal and replacement clearance, in-the-way-removals, the possibility of maintenance induced damage, special tools, soft-dock, tethering, labels, lightning, orientation, orientation arrows, handles, and captive fasteners.

7.5 The P/P/S reviews the architecture used to test the components. This review should be conducted with RAMEs and should cover design provisions for failure detection, isolation, and recovery.

7.6 The P/P/S and RAMEs review the Logistics Support Plan.

7.7 The P/P/S or RAMEs performs the maintainability analysis. If maintenance action time data is available from actual repair or removal and replacement (R&R) simulations, good estimates can be made of the mean-time-to-repair (MTTR). If such data is not available, an appropriate maintainability model can be assumed and some estimate can be made of MTTR.

7.8 RAMEs prepare the Maintainability Analysis Report.

7.9 Engineering Review. Selected P/P/S engineers review the report. Engineers perform a

technical review and provide any needed corrections, or recommend deletions, and/or additions.

7.10 Is the analysis approved? YES: If the P/P/S agrees with the technical content of the report and its findings, the report may be simply revised. NO: If the report is disapproved, the RAME may return to step 7.7 and the entire process for the maintainability prediction analysis may be reviewed. Errors in process will be corrected.

7.11 RAMEs distribute the final (signed off) report and file.

7.12 RAMEs provide instructions and assistance to the P/P/S for developing the Limited Life Items List.

7.13 The P/P/S develops a Preventative Maintenance Plan in response to the limited life items that are found within the system design.

8.0 INSTRUCTIONS – AVAILABILITY ANALYSES

8.1 The P/P/S determines the mission duration and whether the system will be repairable. YES: Proceed with Availability Analysis. NO: Proceed to Reliability Analysis. For non-repairable systems, the P/P/S and RAMEs may select Reliability Prediction Analysis.

8.1.1 RAMEs will use Reliability Prediction. Go to Section A, step 6.1.

8.2 RAMEs: Has a system reliability prediction been performed? YES: Proceed to block 8.2.1. The Reliability Analysis Report will have the reliability block diagrams (RBDs) which can be used to construct the availability model and failure rate data on components which are a major part of the input data for the model. (MTBF = 1/ failure rate) NO: If no Reliability Prediction Analysis has been performed, then we proceed with the Availability Analysis process.

8.2.1 RAMEs review the Reliability Analysis Report.

8.3 The P/P/S and RAMEs review the system design. The P/P/S provides documentation which describes the design and operation of the system and may consist of the Baseline Concept Document, with functional block diagrams, a functional description, drawings, schematics, parts lists, materials, hardware map, specifications, and interface descriptions.

8.4 The P/P/S defines the components needed in the system. This should include: 1.) the definition of what constitutes successful system operation (mission success), 2.) the intended operating environment, 3.) stresses expected on major components during operation, 4.) required operating time for each major component, 5.) functional inputs and outputs for each major component.

8.5 RAMEs estimate the mean-time-between failures (MTBFs).

8.6 The P/P/S and RAMEs draw the reliability block diagrams. These diagrams should depict those components that must operate in series and in parallel (redundant configuration) in order to attain successful operation.

8.7 RAMEs input the MTBF data into the availability model.

8.8 Has a System maintainability analysis been performed? YES: Proceed to block 8.8.1. The Maintainability Analysis Report will have the mean-time-to-repair (MTTR) data on components which is a major part of the input data for the availability model. NO: If no Maintainability Prediction Analysis has been performed, then we proceed with the Availability Analysis process.

8.8.1 RAMEs: Review analysis and extract MTTR data.

8.9 RAMEs: Based on a consideration of component (ORU/LRU) accessibility, alignment, removal and replacement clearance, in-the-way-removals, and other factors such as effectiveness of fault detection and isolation, an estimate of component MTTRs is made. Such estimates may be superceded if more realistic maintenance action time data is available from actual repair or removal and replacement (R&R) simulations.

8.10 RAMEs input the MTTR data into the availability model.

8.11 Are we to estimate only inherent Availability? YES: This type of availability computation only requires the model and the MTBF /MTTR inputs which we now have. We proceed to step 8.15. NO: We need to compute operational availability. Proceed to step 8.13.

8.12 Has a prior estimate of logistics parameters been made? Examples of needed inputs are mean-logistics delay time (MLDT) [time to provide a spare from spare supply to point of required maintenance action], spares re-supply interval, and time required to procure a spare for unplanned events. YES: Proceed to step 8.12.1. NO: Proceed to step 8.13.

8.12.1 RAMEs: Logistics parameters are obtained from Logistics Support Analysis (LSA) report or from preliminary calculations made by Logistics Engineering.

8.13 RAMEs: Work with Logistics Engineering to make the best possible estimate of logistics parameters with available information.

8.14 RAMEs: Inputs the logistics data into the Availability Model.

8.15 RAMEs: Performs the Availability computations based on the availability model. This may be done by computer or manually.

8.16 Maintainability Assurance compiles results and evaluates findings.

8.17 IPT Review: The Availability Analysis is submitted to the IPT for review. This review enables the IPT to take the analysis into account in the development of their designs and other analysis products. The IPT also reviews the analysis with respect to the design to determine if additions, corrections, or deletions are recommended.

8.18 Is a trade study needed? YES: The system does not meet its availability goal. A trade study should be performed to determine what changes in system parameters are needed to achieve the availability goal. NO: The system has met its availability goal.

8.19 RAMEs write a preliminary report. The report shows the results of the availability study. It will discuss risk and make recommendations to improve operational availability.

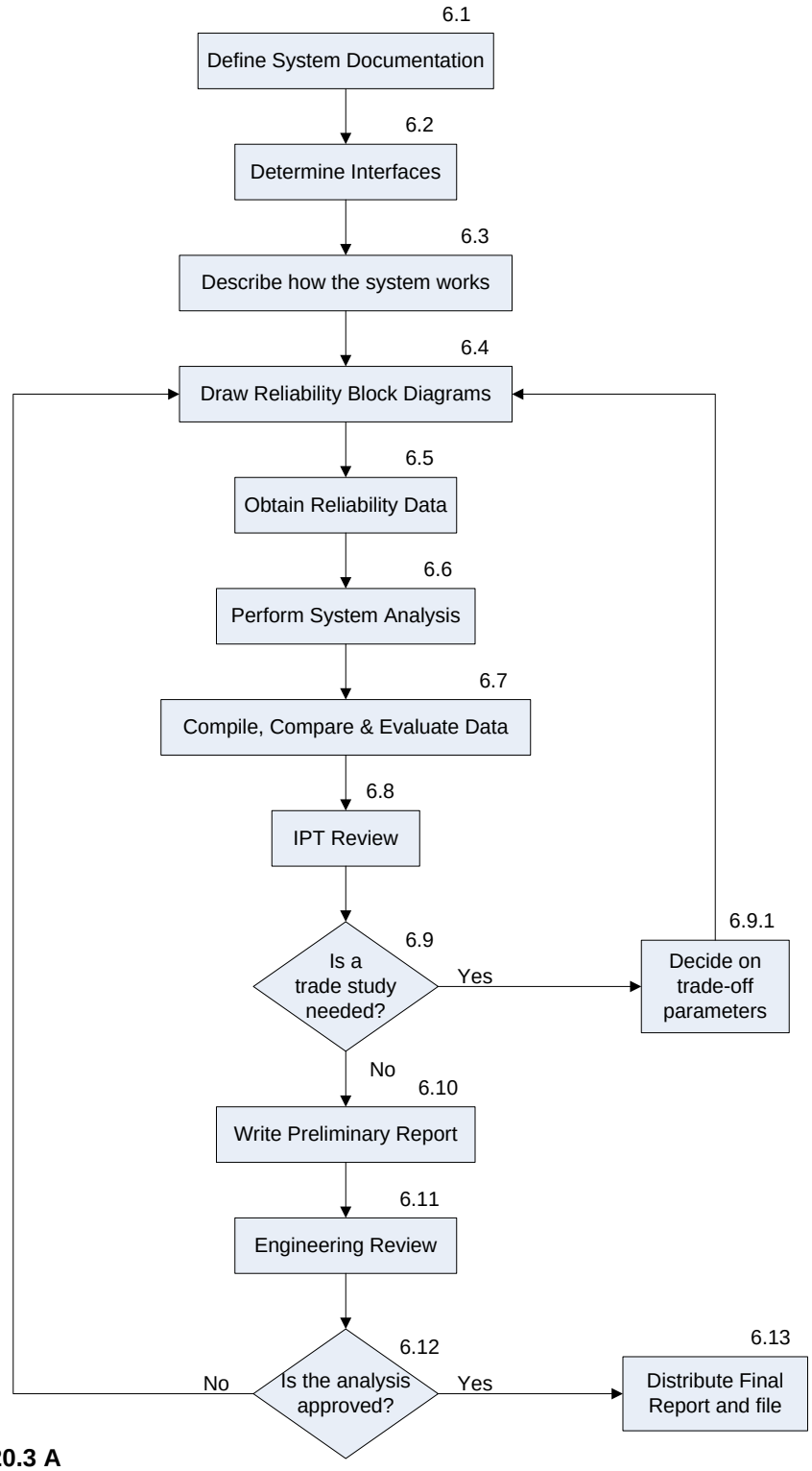
8.20 Engineering Review. Selected P/P/S engineers review the analysis report. Engineers perform a technical review and note any needed corrections, or recommend deletions, and/or additions.

8.21 Is the analysis approved? YES: If the P/P/S agrees with the technical content of the report and its findings, the report may be simply revised. NO: If the report is disapproved, the RAMEs may return to step 8.6 and the entire process for the availability prediction analysis may be reviewed. Errors in process will be corrected.

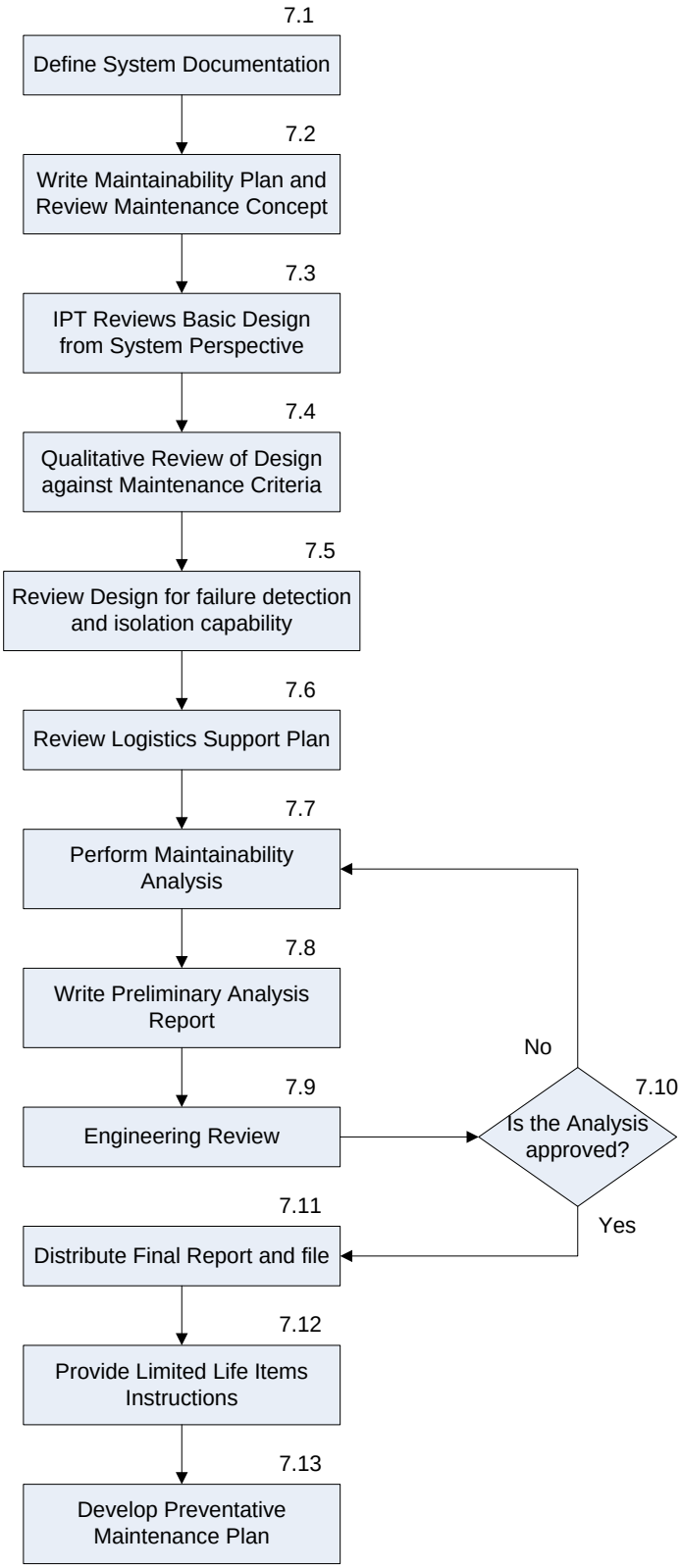
8.22 The approved final report (signed off) is distributed and filed.

9.0 FLOW DIAGRAMS

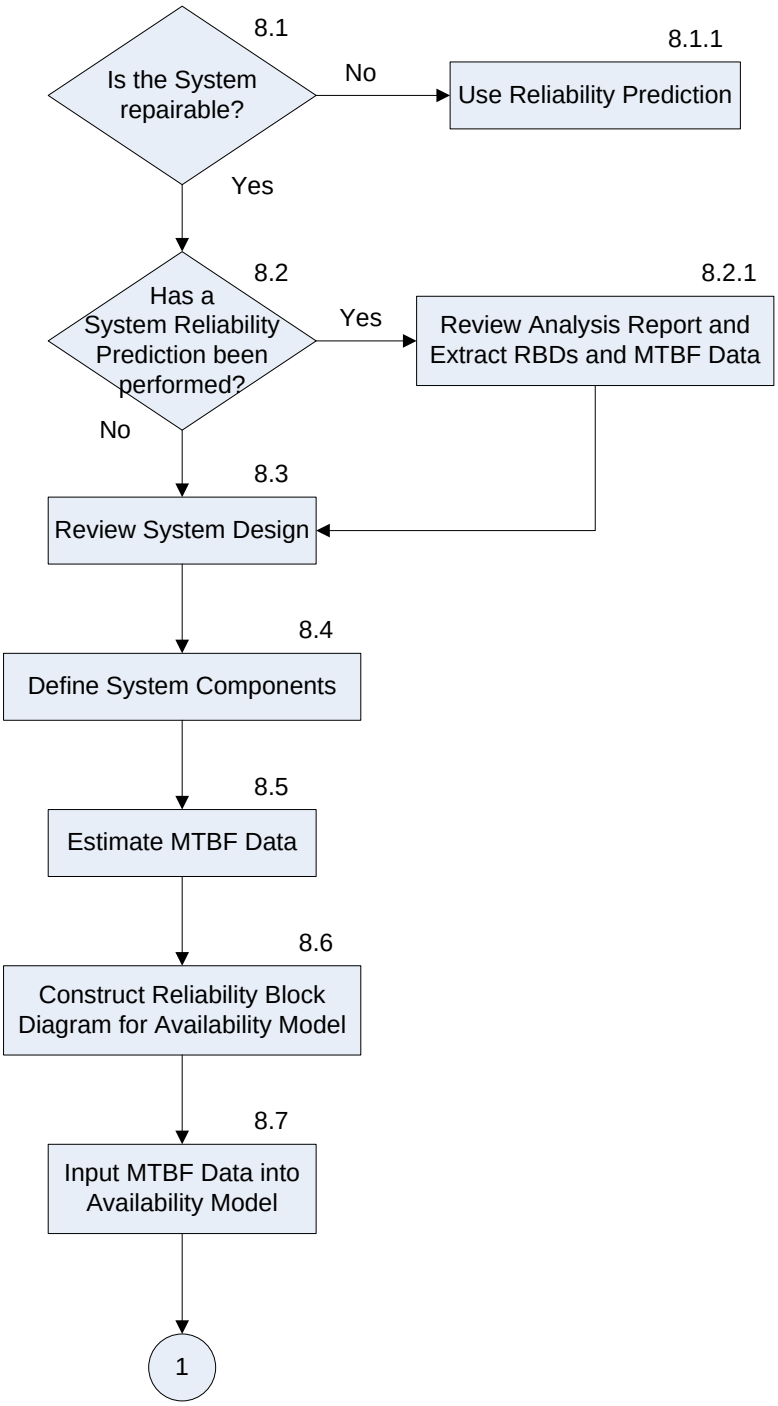
Reliability Prediction Flow Chart



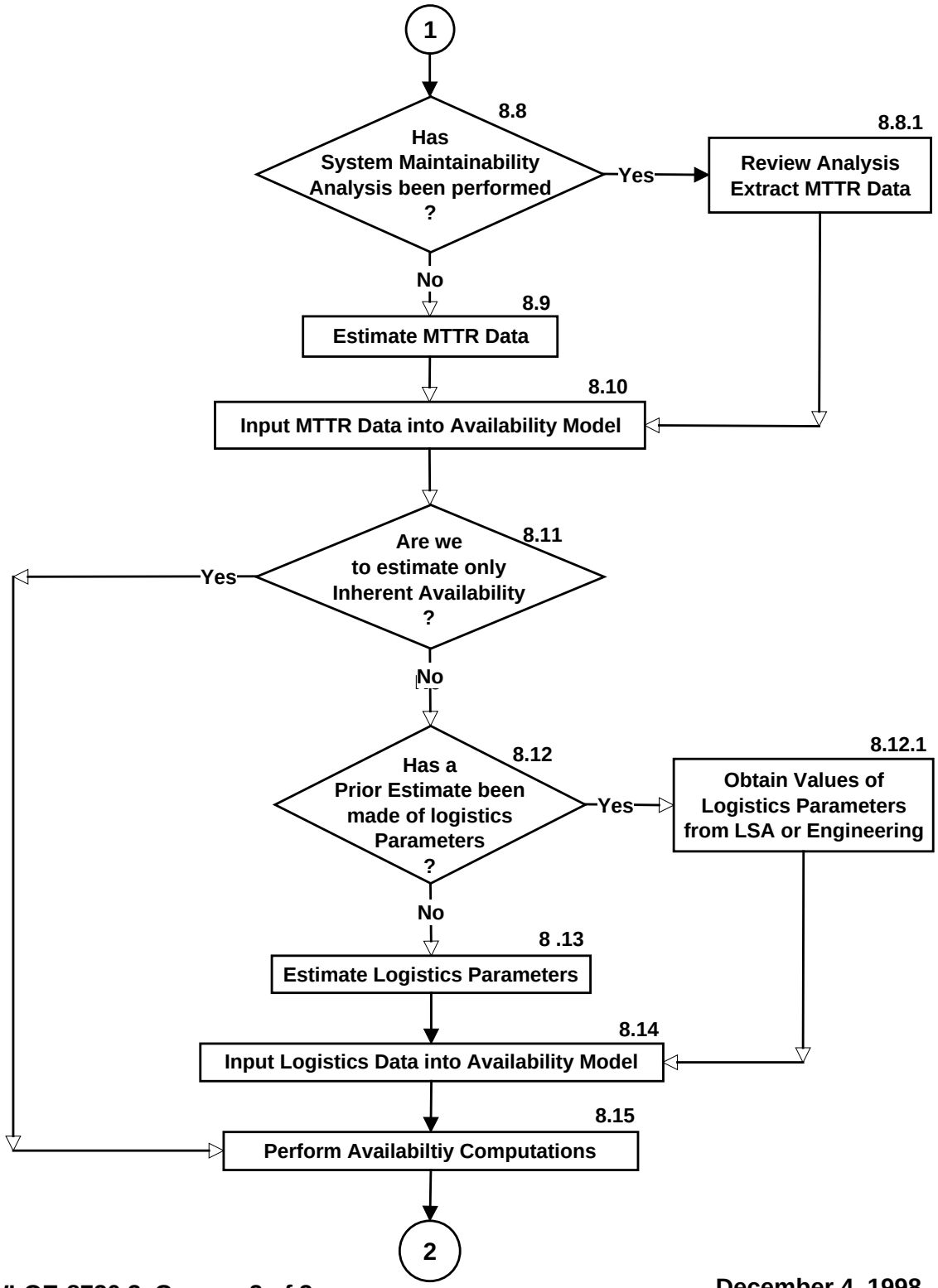
Maintainability Assessment Flow Chart

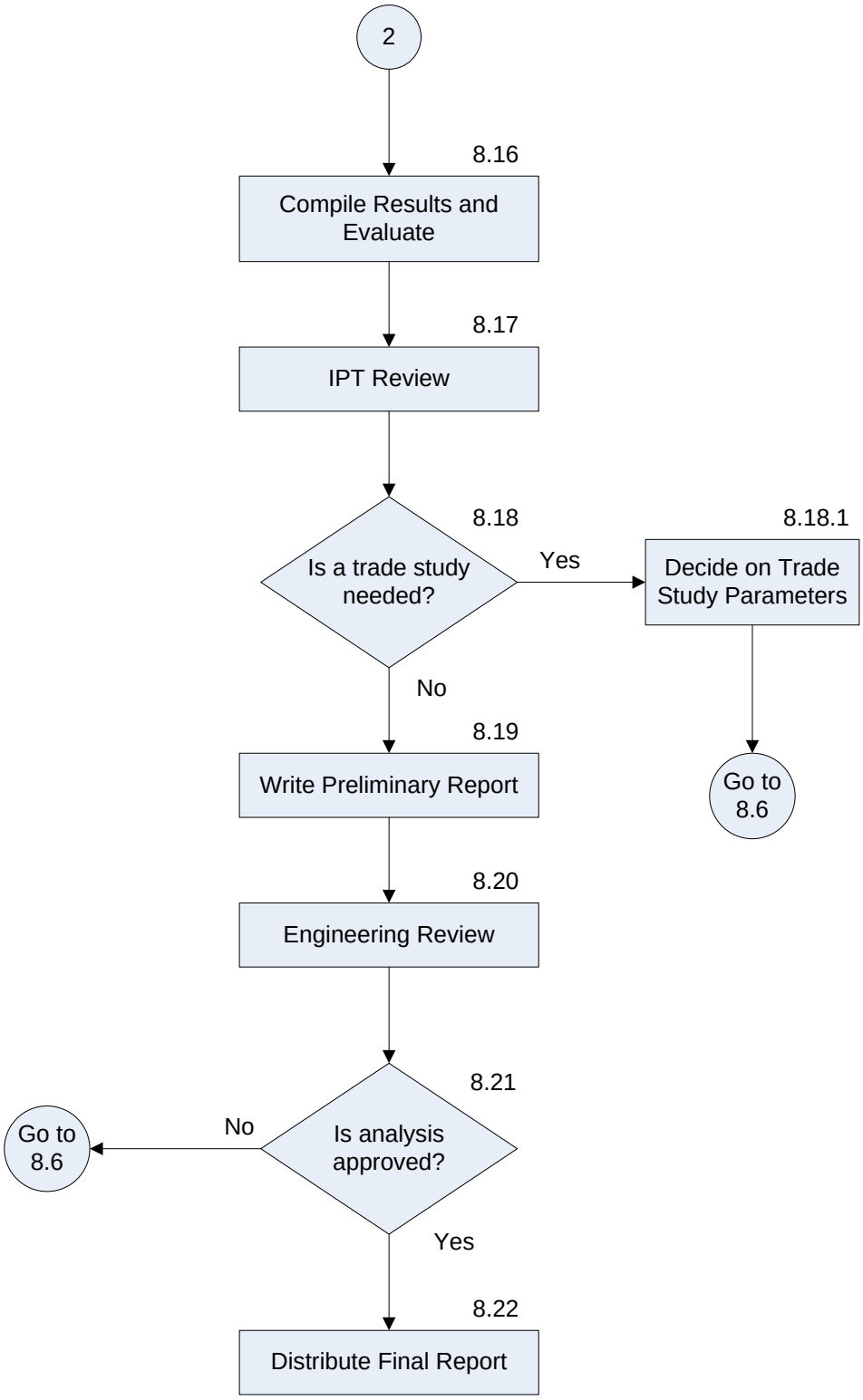


Availability Analysis



GLWI-QE-8720.3 C, page 1 of 3


1
8.8
Has System Maintainability Analysis been performed ?
Yes
8.8.1
Review Analysis Extract MTTR Data
No
8.9
Estimate MTTR Data
8.10
Input MTTR Data into Availability Model
8.11
Are we to estimate only Inherent Availability ?
Yes
No
8.12
Has a Prior Estimate been made of logistics Parameters ?
Yes
8.12.1
Obtain Values of Logistics Parameters from LSA or Engineering
No
8 .13
Estimate Logistics Parameters
8.14
Input Logistics Data into Availability Model
8.15
Perform Availabiltiy Computations
2



GLWI-QE-8720.3 C, page 3 of 3