



RDECOM



TECHNICAL REPORT NO. TR-2011-24

DESIGN FOR RELIABILITY HANDBOOK

AUGUST 2011

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

**US ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY
ABERDEEN PROVING GROUND, MARYLAND 21005-5071**

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YYYY) AUGUST 2011		2. REPORT TYPE Technical Report		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE DESIGN FOR RELIABILITY HANDBOOK				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Matthew J. Rhoads				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Director US Army Materiel Systems Analysis Activity 392 Hopkins Road Aberdeen Proving Ground, MD				8. PERFORMING ORGANIZATION REPORT NUMBER TR-2011-24	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The Design for Reliability (DFR) process blends aspects of statistics, probability and reliability theory, and engineering analysis throughout a product lifecycle to evaluate, predict, and verify the application of robust design. Through application of DFR practices, the demand for highly-reliable systems can be met while insuring that the latest methods for the assessment of robust design and reliability risk-management are properly addressed. This document aims to discuss, in brief, the mathematic and engineering approaches involved in the DFR process. The topics covered introduce the stepped approach to analyzing materiel from conceptual design through production.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAME AS REPORT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK.

CONTENTS

	Page
LIST OF FIGURES	vi
LIST OF TABLES	vii
ACKNOWLEDGEMENTS	viii
LIST OF ACRONYMS	ix
1. EXECUTIVE SUMMARY	1
2. INTRODUCTION	2
2.1 Motivation.....	2
2.2 Scope.....	2
2.3 Organization.....	2
3. BLOCK DIAGRAMMING AND RELIABILITY ALLOCATION.	4
3.1 Overview.....	4
3.2 Reliability Allocation.....	5
4. FAULT TREE ANALYSIS	7
4.1 Overview.....	7
4.2 Fault Tree Development.	7
4.2.1 Top Level.....	7
4.2.2 Modeling Events.....	7
4.2.3 Bottom Level.	8
4.3 Assigning Allocations.....	8
4.4 Benefits.....	8
4.4.1 Design Issues.	8
4.4.2 Root Cause Analysis.....	8
4.4.3 Demonstrated vs. Allocated.....	9
4.4.4 Tradeoffs.....	9
5. RELIABILITY GROWTH TESTING	10
5.1 Overview.....	10
5.2 Reliability Growth via Engineering Approaches.....	11
5.3 FRACAS.....	11
6. FMEA/FMECA.....	13
6.1 Overview.....	13
6.2 Inputs.....	13
6.3 Risk Priority Numbers	13
6.4 Criticality Analysis Method.....	15
6.4.1 Quantitative Criticality Analysis Method.....	15
6.4.2 Qualitative Criticality Analysis Method.....	15
6.5 Post Identification Investigation	15
6.6 Process Benefits	15

7.	PRODUCT LIFECYCLE TESTING METHODS	16
7.1	Accelerated Life Testing	16
7.1.1	Overview	16
7.1.2	Qualitative ALT	16
7.1.3	Quantitative ALT	16
7.2	Highly Accelerated Life Testing	17
7.2.1	Approach	17
7.2.2	Failure Analysis	17
7.2.3	Corrective Action Verification	18
7.2.4	Database Management	18
7.2.5	Test Processes/Procedure	18
8.	STRESS SCREENING METHODS	20
8.1	Highly Accelerated Stress Screening	20
8.1.1	Overview	20
8.1.2	Approach	20
8.1.3	Precipitation	20
8.1.4	Detection	20
8.1.5	Failure Analysis	21
8.1.6	Corrective Action Verification	21
8.1.7	Database Management	21
8.2	Environmental Stress Screening	21
8.2.1	Overview	21
9.	PHYSICS OF FAILURE	22
9.1	Mechanical PoF Approach	23
9.1.1	The Dynamics Modeling Process	23
9.1.2	Finite Element Method	23
9.1.3	Fatigue and Fracture	24
9.1.4	Testing	25
9.2	Electronic PoF Approach	26
9.2.1	Operational Environment	26
9.2.2	Software	27
9.2.3	Modeling the CCA	27
9.2.4	Modal and Random Vibration Response Analysis	27
9.2.5	Thermal Overstress Analysis	27
9.2.6	Shock Response and Survivability Assessment	27
9.2.7	Vibration Fatigue Life Assessment	27
9.2.8	Thermal Fatigue Life Assessment	28
9.2.9	Combined Fatigue Life Assessment	28
9.2.10	Design to Reduce Vibration/Shock Failures	28
9.2.11	Design to Reduce Temperature Cycling Failures	30
9.2.12	Design to Reduce Thermal Overstress Failures	31
9.3	Summary	32
10.	SOFTWARE-IN-SYSTEMS RELIABILITY	33

10.1	Reliability Block Diagrams and Reliability Allocation	33
10.2	Software Reliability Growth Testing.....	34
10.3	Software Reliability Testing	37
10.4	Software FMECA	37
10.5	Fault Tree Analysis for Systems Containing Software.....	38
11.	SYSTEM AND SUB-SYSTEM LEVEL PROTOTYPING.....	40
11.1	Background.....	40
11.2	Benefits of Prototyping Early in the Design Phase.....	40
11.3	Rapid Prototyping.....	41
11.4	Design Verification Testing.....	41
11.5	Interface Testing.....	41
12.	TEST AND EVALUATION	42
12.1	Test and Evaluation.....	42
12.2	Testing.....	42
	12.2.1 Environmental Stress Screening.....	42
	12.2.2 Accelerated Life Testing.....	42
	12.2.3 Design of Experiments.....	42
	12.2.4 Reliability Qualification Testing.....	43
	12.2.5 Reliability Production Testing	43
12.3	Physics of Failure and Testing cooperation.....	43
	12.3.1 System Level Testing.....	44
	12.3.2 Survey Testing.....	44
	12.3.3 Component Analysis Testing.....	44
	12.3.4 Reliability Enhancement Testing.....	44
13.	CORRECTIVE ACTIONS AND FOLLOW ON TESTING	46
13.1	Analytical Correction.....	46
13.2	Intuition or Determination	46
13.3	Reduction of Test-Fix-Test.....	46
13.4	Support to Follow-On Testing	46
14.	SUMMARY	47
15.	NOTES.....	48
15.1	Intended use.....	48
15.2	Superseding information.....	48
15.3	Subject term (Keyword listing).....	48
15.4	Changes from previous issue: Previous Issue Unavailable.....	48
APPENDIXES		
	A - SIX COLUMN MATRIX.....	A-1

LIST OF FIGURES

Figure No.	Title	Page
1	Reliability Block Diagram.	4
2	RBD in a Series Configuration.	4
3	RBD in a Parallel Configuration.	5
4	RBD in Standby Configuration.	5
5	Typical Fault Tree Construct.	7
6	Sub-Level Development of the Fault Tree Diagram.	8
7	Reliability Growth Testing Process.	10
8	Mechanical PoF overview.	23
9	Selection of a Software Reliability Growth Model.	36
10	Reasons to Test Software.	37
11	Sample Software FMECA Worksheet.	38
12	Potential "Clue List" for Software Problems.	39
13	Robust Design Cycle.	40

LIST OF TABLES

Table No.	Title	Page
1	FMECA Process Checklist.	14

ACKNOWLEDGEMENTS

The US Army Materiel Systems Analysis Activity (AMSAA) recognizes the following individuals for their contributions to this report.

The author(s) are:

Matthew J. Rhoads, Logistics Analysis Division, LAD

The author wishes to acknowledge the contributions of the following individuals for their assistance in the creation of this report:

James Arters, LAD

Gary Drake, LAD

Ed Habtour, LAD

Brian Hairfield, LAD

Shelley Hartman, U.S. Army Research Laboratory

Nate Herbert, LAD

David Mortin, Ph.D., LAD

Alexander Karahalis, LAD

Marguerite Shepler, LAD

Martin Wayne, LAD

Rebecca Wentz, LAD

Troy Wilke, Commanding General's Initiatives Group

LIST OF ACRONYMS

AMSAA	US Army Materiel Systems Analysis Activity
LAD	Logistics Analysis Division
SR	Special Report
TR	Technical Report
DFR	Design for Reliability
AES	Auger Electronic Spectroscopy
ALT	Accelerated Life Testing
ANOVA	Analysis of Variance
CA	Corrective Actions
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CCA	Circuit Card Analysis
CSCI	Computer Software Configuration Items
CTE	Coefficient of Thermal Expansion
DOE	Design of Experiments
EDAX	Energy Dispersive Analysis
ESS	Environmental Stress Screening
FD	Failure Definition
FEA	Finite Element Analysis
FEM	Finite Element Method
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes, Effects, and Criticality Analysis
FPRB	Failure Prevention and Review Board
FRACAS	Failure Reporting and Corrective Action System
FTA	Fault Tree Analysis
HALT	Highly Accelerated Life Testing
HASS	Highly Accelerated Stress Screening
HAST	Highly Accelerated Stress Test
LRIP	Low Rate Initial Production
M&S	Modeling and Simulation
MEFs	Mission Essential Functions
MP	Mission Profile
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
O&S	Operations and Support
OEM	Original Equipment Manufacturer
OMF	Operation Mission Failure
OMS	Operational Mode Summary
PDR	Preliminary Design Review

PMs	Product Managers
PoF	Physics of Failure
PSD	Power Spectral Density
PWB	Printed Wiring Board
RBD	Reliability Block Diagram
RCA	Root Cause Analysis
RET	Reliability Enhancement Testing
RGT	Reliability Growth Testing
RPN	Risk Priority Number
SA	System Abort
SC	Scoring Criterion
SEM	Scanning Electron Microscope

DESIGN FOR RELIABILITY HANDBOOK

1. EXECUTIVE SUMMARY

The Design for Reliability (DFR) process blends aspects of statistics, probability and reliability theory, and engineering analysis throughout a product lifecycle to evaluate, predict, and verify the application of robust design. Through application of DFR practices, the demand for highly-reliable systems can be met while insuring that the latest methods for the assessment of robust design and reliability risk-management are properly addressed.

This document aims to discuss, in brief, the mathematic and engineering approaches involved in the DFR process. It is designed to provide the next level of detail following the current GEIA-STD-0009 “Reliability Program Standard for Systems Design, Development, and Manufacturing”, which covers the “what to do” of design and building inherently reliable systems. While not directly intended to be a step-by-step guide, the details contained here within introduce the stepped approach to analyzing materiel from conceptual design through production. Incorporation of the applicable design processes will help guarantee a robust final design while limiting design lifecycle time and cost.

Due to the brevity of this report, detailed development of underlying theory procedural steps is not provided. More extensive details are available in the cited literature or through the authors of this document. Comments, suggestions, or questions on this document should be addressed to the U.S. Army Materiel System Analysis Activity (AMSAA), ATTN: RDAM-LR, 392 Hopkins Road Aberdeen Proving Ground MD, 21005-5071, or emailed to the AMSAA Webmaster, apgr-amsa-akwebmaster@conus.army.mil.

2. INTRODUCTION

2.1 Motivation. This document was developed to address the appropriate mathematical and engineering practices during the materiel acquisition process for new military systems. Historically, these systems have required emergent technologies, and as such have presented a challenge in the upholding of system reliability standards. Thus, the guide aims to address the challenges presented through the application of techniques used to understand reliability concerns at the fundamental level, develop solutions to concerns as they arise, and validate the solutions as the design matures. The reliability concepts and methodologies presented within this guide have evolved from accepted commercial practice and actual application to Army, Marine, Navy and Air Force systems during their associated design and re-design lifecycles.

2.2 Scope. This guide is written as an overview for both the manager and the analyst. It extends coverage of the DFR process topics identified in GEIA-STD-0009 and expands upon the mathematical and engineering process steps required to ensure robust design. While this manual is intended to provide a general understanding of the concepts and principles required, and serve as an outline to robust design, it is not meant to be employed without project specific tailoring. When used in conjunction with project specifications, it should serve as a basis for identification and planning of the appropriate process steps that should be utilized during the design process thus improving the system reliability of fielded systems.

2.3 Organization. While the handbook has been organized by section title, it should be noted that many of the design practices covered are applicable at multiple stages of the design process. The six column matrix designed to relate the inputs and outputs of GEIA-STD-0009 is provided in Appendix A - SIX COLUMN MATRIX for review.

A typical design lifecycle begins with definition of the initial requirements, the operational and environmental loads on the system, assemblies, subassemblies, and components. The initially proposed system design is laid out via block diagramming. This leads to system reliability model creation to investigate the interconnectivity of assemblies and components in turn allowing for the examination of cause and effect relationships inherent in complex multi-level systems.

The utilization of block diagramming also helps in the determination of various failures points within the design. Examination of these failure points and relationships through top-down Fault Tree Analysis provides a system level view of potential loss of functionality. In addition, block diagramming facilitates component level failure mode analysis of system reliability using a Failure Mode and Effect Criticality Analysis (FMECA) or Failure Mode and Effect Analysis (FMEA) approach.

Early in the design processes, Highly Accelerated Life Testing (HALT) is utilized to expose early prototypes and existing components to the full range of expected operating conditions, within a controlled environment. Any deficiencies identified during HALT testing are inspected using a Physics of Failure (PoF) approach or are addressed directly in the refinement of the conceptual design. At this phase, PoF Computer Aided Design (CAD) practices including dynamic modeling and simulation, finite element stress and heat transfer

analysis, and component fatigue analysis toolsets are utilized to predict failure mechanisms and conduct reliability assessments on the proposed design and any subsequent design revisions.

As the iterative design process progresses, early prototype quality testing is employed to validate design changes and assumptions as well as the results derived from HALT and PoF analysis. Using the iterative DFR process provides benefits in reduction of early-on physical testing and traditional test-fix-test cycles, while ensuring that the reliability level of the Preliminary Design Review (PDR) design candidate is equal to or exceeds the minimum level identified by reliability growth modeling. Estimation of the design candidate's initial reliability can be done through a combination of modeling and simulation along with lower level testing. Milestone B requirements are typically met at this point, and the design process moves to the complete system prototype phase.

Post Milestone B, complete system prototypes experience exhaustive testing to capture both hardware and software reliability metrics. Reliability growth testing is conducted in parallel with HALT, Accelerated Life Testing, and Environmental Testing to provide engineering confirmation and feedback data for mathematical modeling. Information captured from previous PoF and HALT analysis is leveraged during test to ensure that any areas of concern are properly instrumented and tracked. Training strategies are also investigated for comprehension and effectiveness.

Corrective actions are identified to mitigate the reliability deficiencies that arise during the test phase. These actions are typically addressed via engineering redesign of mechanical components, software recoding, or adjustments to training practices. In the case of engineering redesign, PoF mechanisms assist in root cause analysis and provide insight for prototype design revision. The PoF toolset is the same as that utilized pre-Milestone B and application again aids in the reduction of test-fix-test cycling. Accelerated tests can also be used at this point to quickly verify corrective actions. The subsequent reduction in time between failure and robust redesign is a large benefit of the enhanced iterative design process. As design testing proceeds and interim reliability goals are demonstrated through test results, the prototype design moves towards Low Rate Initial Production (LRIP) level maturity.

As LRIP begins, Highly Accelerated Stress Screening (HASS), Environmental Stress Screening (ESS) or the like is implemented to ensure production line reliability. LRIP assets enter Operational Test and Evaluation (OT&E) for verification that final designs meet operational reliability requirements. Engineering rework, software recoding, and training practice corrective actions are identified for any failure modes that are identified through HASS, ESS, or operational testing. PoF and HALT techniques are employed to expedite the time between any potential failures and corrective actions. They also help to reduce the length and complexity of any necessary follow-on test and evaluation. This reduces time between LRIP production and a move to full rate production and fielding.

3. BLOCK DIAGRAMMING AND RELIABILITY ALLOCATION.

3.1 Overview. For a given system, models are often used to describe the relationship between the system components in order to determine the reliability of the system as a whole. A common and useful way to model these interconnected relationships is the utilization of Reliability Block Diagrams (RBD). An RBD is a success-oriented network drawing and calculation tool used to model specific functions of complex systems by using a series of images (blocks). When used to model a system, each component within the system is represented by a block and the connections between the blocks are used to indicate that each component is properly performing its intended function. As seen from Figure 1, if a connection exists between the two end points (a,b) of the diagram, it is said that the system is performing its intended function or that some specified failure mode is not occurring. Once the blocks are configured in the proper form the hazard rate (instantaneous failure rate), mean time between failures (MTBF), mean time to repair (MTTR), reliability, and availability of the system can be calculated.

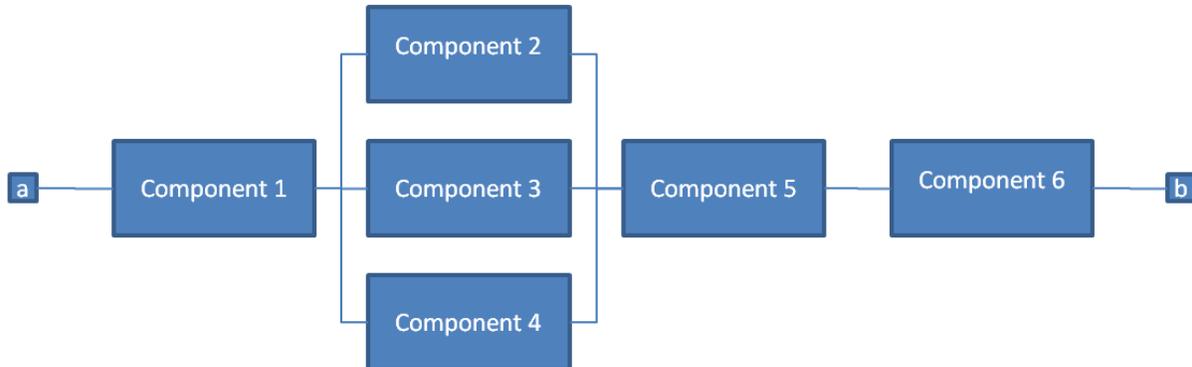


Figure 1. Reliability Block Diagram.

RBD can take a number of different forms allowing for testing for different item configurations and system loads. The basic forms of RBD include components placed in series, parallel, stand-by, load-sharing or complex. As seen in Figure 2, an RBD in series is represented by each block placed in a straight line sequence. As with any RBD, as long as a single connection between the end points exists, the system is performing its intended function.

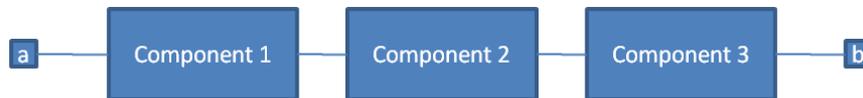


Figure 2. RBD in a Series Configuration.

In a series configuration, if any single component fails, it would result in the end points being disconnected and the system failing to perform its function. Thus, for this system to perform its intended mission, every component must succeed during the mission time.

An RBD with components in a parallel configuration is represented by Figure 3. In this configuration, as long as at least one block is operational, the system is performing its intended function. Parallel configurations represent active redundant systems where if one component fails a back-up is already in place.

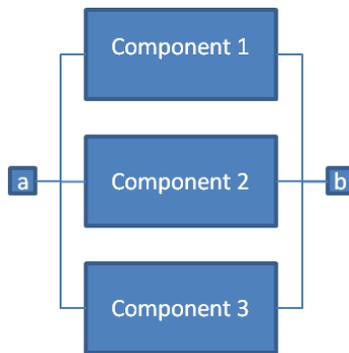


Figure 3. RBD in a Parallel Configuration.

While parallel configurations offer active redundancy, a system with a configuration depicted in Figure 4 offers a standby configuration. In the standby configuration, the component has redundant components which are not actively connected but are triggered by a switch. The original component is intended to last for the extent of its life; however, in the event that the component fails prematurely, a switch activates the redundant component to do the job. An example of the standby configuration would be two generators connected to a power grid having only one generator with an active load. If that generator were to fail, the other generator could be activated in its absence.

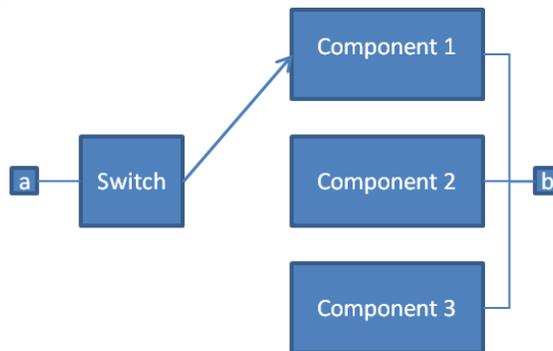


Figure 4. RBD in Standby Configuration.

A load-sharing system is one where the components are arranged in a parallel configuration, but each component equally shares a system's function. An example of this is a set of two identical fuel pumps each producing $x/2$ gallons per hour. If the requirement were that x gallons per hour were required, then both pumps would be required not to fail in order to keep the system operational. In this case, the extra components act to share the overall load of the system rather than acting as an active redundancy.

The final general form of RBD is the complex form. In reality, most systems will not be strictly parallel or series but are often some combination of the two. Figure 1 of the previous page shows a system that is a parallel-series hybrid. These systems can be analyzed by breaking the system into each of the parallel and series modules to determine the effect of failure.

3.2 Reliability Allocation. After the system has been drawn in block diagram form, subsystem and component reliability goals and targets are established. This is a common

practice in the development of complex systems, particularly when different design teams or subcontractors are involved. Reliability allocation involves setting reliability objectives for components or subsystems in order to meet a system reliability objective and should occur in the initial stages of design or prior to designing major system upgrades. The simplest method for allocating reliability is to distribute the reliability objective uniformly among all the subsystems or components. While uniform allocation is easy to calculate, it is generally not the best way to allocate a reliability objective. The "best" allocation of reliability would take into account the cost or relative difficulty of improving the reliability of different subsystems or components.

The RBD model of a system can be used to optimize the allocation of reliability to different components in order to meet a reliability specification while considering the cost of the allocation. This allows the design team to focus their reliability efforts into the least expensive options for increasing the overall system reliability to meet the requirements. The allocation distributes reliability of subsystems and individual components into more critical blocks or bottlenecks in reliability which will help optimize the best combination of component reliability improvements that meet the intended goals and at sufficient allocated costs.

Reliability allocation usually starts from past experience and is first performed at a higher level of subsystems instead of lower levels such as components sourced from different vendors. This level of detail is more appropriate during the first stages of design. It is not efficient to develop a detailed design and then have to redesign and reallocate reliability if the initial allocation is not achievable. The assignment of reliability values between the components can be made based on the complexity, criticality, estimated achievable reliability, or whichever factor the engineering team performing the analysis deems important.

Many benefits exist from RBD analysis. It allows the maximization of costs and design benefits in allocation; it provides a realistic view of subsystem performance required to meet system objectives; it shows the most cost effective areas for design improvements; and avoids putting design efforts into subsystems that may not gain any additional reliability by improvements. RBD analysis is an essential part of DFR and should be performed early in the design of every system.

4. FAULT TREE ANALYSIS

4.1 Overview. Fault Tree Analysis (FTA) is a logical, top-down method aimed at analyzing the effects of initiating faults and events upon a complex system. It utilizes a block diagram approach that displays the state of the system in terms of the states of its components. As such, FTA is a systematic methodology for defining a specific undesirable event (normally a mission failure) and determining all the possible reasons that could cause the event to occur. Development tasks are typically assigned to engineers having a good understanding of the interoperability of the system and subsystem level components.

4.2 Fault Tree Development. The Fault Tree should be developed during the initial design phase of the system acquisition process. The top level events in the Fault Tree are typically mission essential functions (MEFs) of the system, which should be defined in the system's Failure Definition / Scoring Criteria (FD/SC). If a component failure results in a loss of one of these mission essential functions, then that failure would be classified as an Operation Mission Failure (OMF), System Abort (SA) failure, or other applicable nomenclature for failures that count against the reliability requirement of the system.

4.2.1 Top Level. The Fault Tree is built from the top-down and uses a graphic diagram to model the pathways within a MEF that can lead to a foreseeable, undesirable failure. For illustration, Figure 5 shows the four MEFs at the top level for a sample tank system. This system must have the ability to move, shoot, protect, and communicate to the levels specified in the FD/SC. If any MEF is compromised due to a failure on the system, then the system is in a down status and cannot perform its mission. The idea behind the Fault Tree is to break down each one of the MEFs further and further until all failure causes of components and subcomponents are captured.

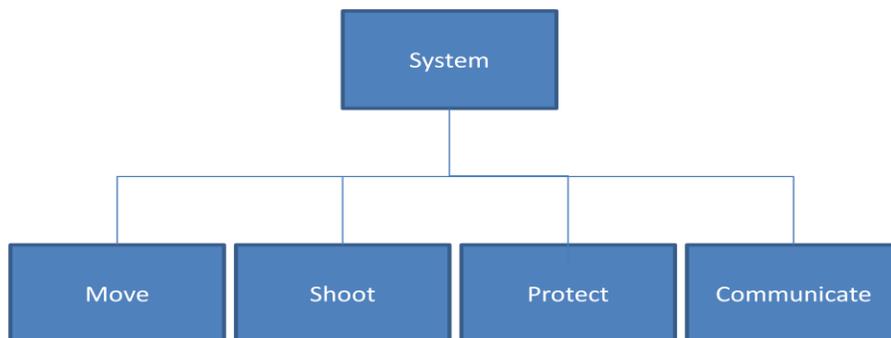


Figure 5. Typical Fault Tree Construct.

4.2.2 Modeling Events. The pathways of Figure 5 interconnect contributory events and conditions using standard logic symbols (i.e. AND, OR, etc). The basic constructs in a Fault Tree diagram are the events and gates, where the events are the ways in which subcomponents may fail, and the gates are the AND/OR conditions.

To continue building off the Fault Tree begun in the sample depicted in Figure 5, one must then find the next lowest events that would cause a MEF to be lost. For example, loss of the Move MEF could be attributed to events such as: (1) loss of engine power, (2) loss of forward drive, (3) thrown track, (4) broken suspension, etc. Obviously, if any one of these events occurred, the MEF would be lost, therefore such failure modes are attached to the Move MEF with an OR gate. Figure 6 illustrates the breakdown of the Move MEF into the next lowest level.

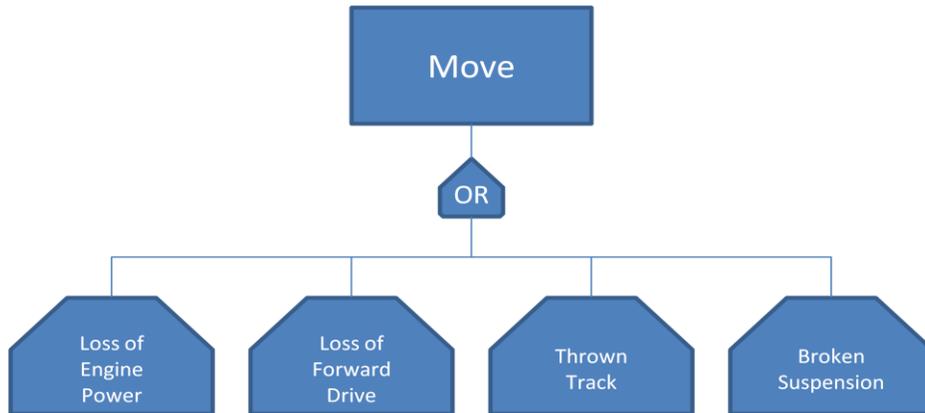


Figure 6. Sub-Level Development of the Fault Tree Diagram.

4.2.3 Bottom Level. The next step in the construction of the Fault Tree is to break out and depict the causes for the failure events as depicted in Figure 6 (loss of engine power, etc). This process is conducted in repeated fashion until the bottommost blocks represent the actual failed component or the operating conditions that caused the eventual mission failure.

4.3 Assigning Allocations. Once the Fault Tree is developed to the greatest detail possible, reliability allocations are assigned to the lowest-level components. The allocations at the component level can be determined by a number of methods. One method is to use data taken from the component while it was used on any other analogous system. Another method is to use supplier data. These allocations, in turn, get rolled-up into the next higher level to determine the allocation of the subsequent level. Continuing this roll-up of allocations eventually leads to a system level reliability allocation.

4.4 Benefits. There are many benefits of developing and analyzing a Fault Tree for a complex system as discussed in the following four sub-sections.

4.4.1 Design Issues. One benefit of the Fault Tree analysis is the ability to identify possible system reliability issues at the time of initial design. By examining the Fault Tree and the interaction between components, an engineer can typically identify potential failure modes that may adversely affect reliability. Resultantly, design changes may be proposed early-on to address concerns over initial system reliability.

4.4.2 Root Cause Analysis. Another benefit is that the Fault Tree can be used to assist with identifying the root cause of a failure observed during test. For example, if the engine failed to start on the system, the engineer may utilize the Fault Tree to find the root cause of

failure based on the data that was captured at the time of failure or by obtaining the actual parts themselves.

4.4.3 Demonstrated vs. Allocated. Fault Tree analysis also provides the ability to compare demonstrated reliability of a component to the allocated reliability of the component. If there is a shortfall in the reliability of a component, then it can be seen as a potential candidate for redesign in order to improve the component level of reliability such that the component meets the previously allocated level.

4.4.4 Tradeoffs. Utilizing a Fault Tree also provides the engineers the ability to study the effect of typical engineering tradeoffs. For example, if time, money, and resources are constrained, then only the redesigns that provide the biggest reliability improvement will be considered for a system. Conducting a Fault Tree analysis allows the engineer to see the quantitative impact component redesigns will have on the overall system reliability.

5. RELIABILITY GROWTH TESTING

5.1 Overview. It is substantially less expensive to uncover, identify and apply fixes to failure modes discovered at the early stages of the system development lifecycle rather than later. Due to the complexity of the failure modes, they can usually only be discovered through multiple means: normal design and development; an informal combination of testing, analyzing and applying fixes; or through a formal reliability growth testing (RGT) program. RGT aims to purposefully surface as many failure modes as possible through rigorous formal testing, analyze the root causes of those failure modes and apply engineered fixes or corrective actions. The main goal of RGT is to enhance reliability by the iterative process of surfacing failure modes, analyzing them, implementing corrective actions (fixes), and testing the ‘improved’ configuration to verify fixes and continue the growth processes by surfacing remaining failure modes.

An overview of the reliability growth process is shown in Figure 7. After a system prototype has been developed and the initial design has matured, the system is ready for RGT. The RGT tests a system using the Operation Mode Summary/Mission Profile (OMS/MP) of the system as a guide. The OMS/MP contains information regarding the expected usage (time), the required capabilities of the system, and specifies what mission the system is required to perform. While performing RGT, it is essential to test the system under a balanced mission profile based on the mean OMS/MP for the system. This allows each of the subsystems to be stressed to the capability required for the expected mission and provides the most accurate estimate of the reliability by allowing each subsystem the proper opportunity to fail.

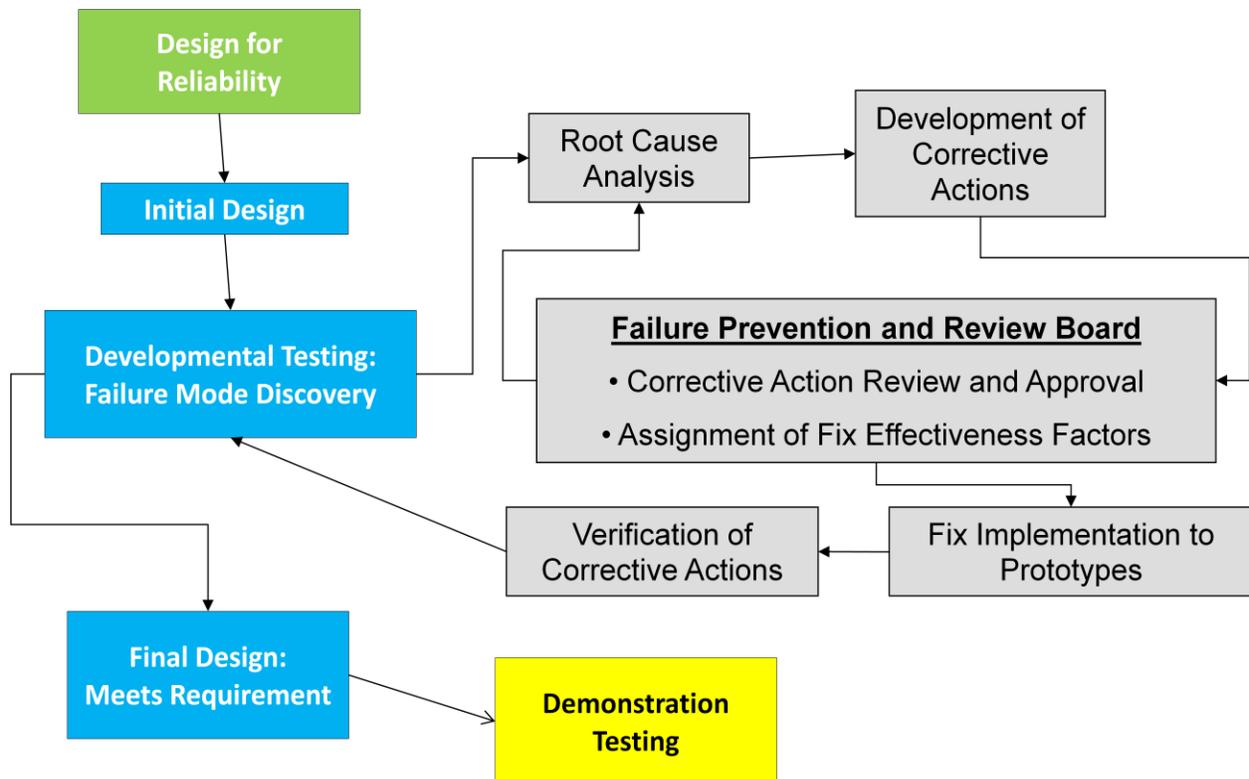


Figure 7. Reliability Growth Testing Process.

Through RGT, it is expected that some of the system components will experience failures. While experiencing a failure is never a desired project outcome, it is important that any failures that occur during RGT are well documented to support a detailed root cause analysis. Data such as which item failed, how it failed, where it failed, what it was doing when it failed, environmental conditions, etc should all be collected using a Failure Reporting and Corrective Action System (FRACAS). The purpose of the root cause analysis is to find the exact reason why the item failed, to the level of detail of the actual design of the item, in order to develop a fix.

Once the cause of the failure has been identified and a proposed fix engineered, the proposed fix is sent to a Failure Prevention and Review Board (FPRB) for review. The FPRB is chaired by the Program Manager and generally incorporates key members from across several areas of the program development process. The board reviews and approves each proposed corrective action and determines the effectiveness of the fix by assigning a fix effectiveness factor. If the corrective action is approved, the fixes are implemented and effectiveness verified. Should the corrective actions not be approved, the root causes are analyzed to determine improvements or other potential fixes.

RGT is an iterative process that has traditionally involved numerous tests, analyze and fix cycles. As such, it is imperative that enough time is scheduled to allow for fixes to be implemented and retested. Typically, the allotted testing time should range between 5 and 25 times the predicted MTBF to ensure that suitable data can be collected. In terms of calendar time, the time allowed should be roughly twice the number of test hours in order to account for downtime. The amount of time required in order to perform the proper testing can necessitate a large upfront monetary investment; however, this cost is generally offset by the large reduction in operation and maintenance cost in the future.

5.2 Reliability Growth via Engineering Approaches. In the course of RGT, failure modes are identified and data regarding each failure are captured. This data can then be analyzed by engineers to determine the precise source of the failure. It is imperative that the engineers find and isolate the true source of failures in order to design a fix that solves the root cause of the problem rather than fixing symptoms.

Root cause analysis can be performed through multiple means ranging from informal trial and error design fixes to detailed Physics-of-Failure (PoF) engineering analyses depending on the complexity of the system and failure. Depicted in Section 9, PoF allows for highly detailed analysis of failure modes through the simulation of design concerns and subsequent corrective actions. PoF analysis helps to reduce time between the traditional test-fix-test iteration and can be used to provide comparative analysis for design fix iterations.

5.3 FRACAS. The Failure Reporting and Corrective Action System (FRACAS) is a closed-loop process whose purpose is to provide a systematic way to report, organize and analyze failure data. Implementation of a FRACAS has increasingly become commonplace within industry. The requirement for implementation of some type of FRACAS within a DoD program was first established in 1985 with MIL-STD-2155. However, in 1995 that standard was reestablished with no changes to content as a handbook, MIL-HDBK-2155, and was

recommended as guidance. Today, multiple software solutions exist that provide all the functionality required of a FRACAS.

Each FRACAS process will capture a number of different elements; however, the following features are generally required at a minimum:

- **Failure Reporting.** Failures and faults that occur during developmental or operational testing or during inspections are reported. The failure report should include identification of the failed item, symptoms of the failure, testing conditions, item operating conditions and the time of the failure.
- **Failure Analysis.** Each reported failure is analyzed to determine the root cause. A FRACAS should have the capability to document the results and conclusions of the root cause analysis.
- **Design Modifications.** Details of the implemented corrective actions for each failure mode should be documented. The precise nature of the design change should be captured as well as date of implementation.
- **Failure Verification.** All reported failures need to be verified as actual failures by repeating the failure or evidence of failure, such as a leak or damaged hardware. This verification needs to be tracked within the FRACAS.

A FRACAS is an essential tool when considering the DFR process, as it provides a systematic closed-loop process for reporting, analyzing and tracking failures through development and testing. Much like RGT, FRACAS should be implemented early on in the system development timeline. Providing detailed failure data from an earlier stage makes it easier and less costly to implement the necessary corrective actions. As system development progresses, newly identified failure modes are limited in the options available for corrective actions and implementation of design revisions is typically more difficult and costly.

6. FMEA/FMECA

6.1 Overview. A failure modes and effects analysis (FMEA) is a procedure in operations management for analysis of potential failure modes within a system, conducted to classify the failure modes by severity or determine of the effect of failures on the system. FMEA provides an analytical approach when dealing with potential failure modes and their associated causes. The identification of potential failure modes and causes provides engineers with the information needed to alter the development/manufacturing process in order to optimize the tradeoffs between safety, cost, performance, quality and reliability. FMEA provides an easy tool to determine which risk has the greatest concern, and thereby what action is needed to prevent a problem before it arises. The development of robust process specifications ensures the end product will meet the predefined reliability requirements.

The failure modes, effects and criticality analysis (FMECA) is an extension of the FMEA. FMECA is a reliability evaluation and design review technique that examines the potential failure modes within a system or lower piece-part/component level, in order to determine the effects of component level failures on total equipment or system level performance. Each hardware or software failure mode is classified according to its impact on system operation success and personnel safety. FMECA uses inductive logic (a process of finding explanations) on a “bottom up” system hierarchy and traces up through the system hierarchy to determine the end effect on system performance. Maximum benefits are seen when FMECA is conducted early in the design cycle rather than after the design is finalized. The checklist found in Table 1 covers all essential steps for the FMECA process.

6.2 Inputs. The FMEA/FMECA requires the following basic inputs:

- Item(s)
- Function(s)
- Failure (s)
- Effect(s) of Failure
- Cause(s) of Failure
- Current Control(s)
- Recommended Action(s)

6.3 Risk Priority Numbers. The analysis procedure utilizes the Risk Priority Numbers (RPNs) and Criticality Analysis methods. MIL-STD-1629A provides guidelines and standards for the requirements and recommended reporting format of FMEAs and FMECAs.

The Risk Priority Number (RPN) method is as follows:

- Rate the severity of each effect of failure.
- Rate the likelihood of occurrence for each cause of failure.
- Rate the likelihood of prior detection for each cause of failure (i.e. the likelihood of detecting the problem before it reaches the end user or customer).
- Calculate the RPN by obtaining the product of the three ratings:
$$\text{RPN} = \text{Severity} \times \text{Occurrence} \times \text{Detection}$$

The RPN can then be used to compare issues within the analysis and to prioritize problems for corrective action.

Table 1. FMECA Process Checklist.

Major Concerns	Impact
Is the system definition/description provided compatible with the system specification?	Inaccurate documentation may result in incorrect analysis conclusions.
Are ground rules clearly stated?	These include approach, failure definition, acceptable degradation limits, level of analysis, clear description of failure causes, etc.
Are block diagrams provided showing functional dependencies at all equipment piece-part levels?	This diagram should graphically show what items (parts, circuit cards, subsystems, etc.) are required for the successful operation of the next higher assembly.
Does the failure effect analysis start at the lowest hardware level and systematically work to higher piece part levels?	The analysis should start at the lowest level appropriate to make design changes (e.g. part, circuit card, subsystem, etc.)
Are failure mode data sources fully described?	Specifically identify data sources, including relevant data from similar systems.
Are detailed FMECA worksheets provided? Do the worksheets clearly track from lower to higher hardware levels? Do the worksheets clearly correspond to the block diagrams? Do the worksheets provide an adequate scope of analysis?	Worksheets should provide an item name, piece-part code/number, item function, list of item failure modes, effect on next higher assembly and system for each failure mode, and a critically ranking. In addition, worksheets should account for multiple failure piece-part levels for catastrophic and critical failures.
Are failure severity classes provided? Are specific failure definitions established?	Typical classes are (see MIL-STD-882D for details): Catastrophic (life/death) Critical (mission loss) Marginal (mission degradation) Minor (maintenance/repair)
Are results timely?	Analysis must be performed early during the design phase not after the fact.
Are results clearly summarized and comprehensive recommendations provided?	Actions for risk reduction of single point failures, critical items, areas needing built-in test (BIT), etc.
Are the results being communicated to enhance other program decisions?	BIT design, critical parts, reliability prediction, derating, fault tolerance.

6.4 Criticality Analysis Method. The Criticality Analysis method, as described in MIL-STD-1629A, consists of two analytical types: quantitative and qualitative.

6.4.1 Quantitative Criticality Analysis Method.

- Define the reliability/unreliability for each item, at a given operating time.
- Identify the portion of the item's unreliability that can be attributed to each potential failure mode.
- Rate the probability of loss (or severity) that will result from each failure mode that may occur.
- Calculate the criticality for each potential failure mode by obtaining the product of the three factors:

$$\text{Mode Criticality} = \text{Item Unreliability} \times \text{Mode Ratio of Unreliability} \times \text{Probability of Loss}$$

- Calculate the criticality for each item by obtaining the sum of the criticalities for each failure mode that has been identified for the item.

$$\text{Item Criticality} = \text{SUM of Mode Criticalities}$$

6.4.2 Qualitative Criticality Analysis Method.

- Rate the severity of the potential effects of failure.
- Rate the likelihood of occurrence for each potential failure mode.
- Compare failure modes via a Criticality Matrix, which identifies severity on the horizontal axis and occurrence on the vertical axis.

6.5 Post Identification Investigation. After the failure modes have been properly prioritized, there are a number of failure analysis techniques to identify the root cause of the failure. The specific technique required to analyze the failure depends on the problem at hand. The use of finite element analysis (FEA) is a well established method. FEA can be used to investigate failures caused from thermal, electromagnetic, fluid and structural working environments. Other failure identification techniques include optical microscopy, electrical testing, scanning electron microscope (SEM), Auger electronic spectroscopy (AES), energy dispersive analysis by x-ray (EDAX) and high resolution stereo x-ray radiography.

6.6 Process Benefits. The design for reliability process benefits from the FMEA/FMECA analysis procedure by identifying potential design problem areas up-front and early. It can contribute to improved designs for products and processes, resulting in higher reliability, better quality, increased safety, enhanced customer satisfaction and reduced costs. After performing FMEA/FMECA, recommendations are made to reduce the consequences of critical failures. This may include selecting components with higher reliability, reducing the stress level at which a critical item operates, or adding redundancy or monitoring to the system.

7. PRODUCT LIFECYCLE TESTING METHODS

7.1 Accelerated Life Testing.

7.1.1 Overview. Traditional life characterization analysis involves inspection time-to-failure data obtained under normal operating conditions for a product, system or component, in order to quantify the life characteristics of the product, system or component. In many situations, and for many reasons, time-to-failure data is very difficult to obtain. This difficulty can often be attributed to issues resulting from the small time period between product design and release and the challenge of testing products that are in continuous use during normal operation conditions. Given this difficulty, and the need to better understand failure modes and life characteristics of the products, ALT (Accelerated Life Testing) attempts to devise methods to force these products to fail at a more rapid rate than that experienced during testing under normal operational conditions. ALT can be divided into two areas: Qualitative ALT and Quantitative ALT.

7.1.2 Qualitative ALT. In qualitative ALT, the failure and failure modes identification is conducted without an attempt to make any predictions as to product life under normal use conditions. Qualitative tests are performed on small samples with the specimens subjected to a single severe level of stress, to a number of stresses or to a time-varying stress such as thermal cycling and vibration. If the specimen survives, it may be considered reliable. Otherwise, corrective actions are taken to improve the product's design and/or production process in order to eliminate the failure cause.

Qualitative ALT testing is primarily used to reveal probable failure modes. The tests quickly reveal the failure modes that will occur during the life of the product under normal use conditions. In general, qualitative tests do not quantify the life span or stress based reliability characteristics of the product under normal operating conditions. However, they do provide valuable information as to the types and level of stresses one may wish to employ during a subsequent quantitative test.

7.1.3 Quantitative ALT. In quantitative ALT, the intent is to predict the life of the product at normal use conditions, from data obtained during an accelerated life test. Unlike the qualitative testing process, quantitative ALT consists of tests designed to quantify the life/reliability characteristics of the component or system under normal use conditions and thereby provide reliability information. Reliability information may include the determination of the probability of failure of the product under use conditions, mean life under use conditions and projected returns. It can also be used to assist in the performance of risk assessments, design comparisons, etc.

Quantitative ALT can take the form of usage rate acceleration or overstress acceleration. For products that do not operate continuously under normal use conditions, the testing rate can be accelerated. This continuously operational environment, defined as the usage rate acceleration form of ALT, helps to instigate failures earlier than testing at normal usage rates. Data obtained through usage acceleration may be analyzed with the same methods used to quantify regular times-to-failure data.

For products with very high or continuous usage, the overstress acceleration form of ALT introduces product to failure by applying stresses that exceed the stresses that a product will encounter under normal use conditions. The times-to-failure data obtained under these conditions can then be used to extrapolate to normal or intended use conditions. Accelerated life tests can be performed at high or low temperature, humidity, voltage, pressure, vibration, etc. in order to accelerate or stimulate the failure mechanisms. They can also be performed at utilizing a combination of these stresses.

7.2 Highly Accelerated Life Testing. Highly Accelerated Life Testing (HALT) is a method aimed at discovering and then improving weak links in the product in the design phase. HALT is performed to precipitate and detect latent defects/weaknesses in early design stages that may, or may not, be uncovered in conventional qualification methods to improve reliability. By simulating the item with stresses beyond what it would normally see in field use, HALT compresses the test time required and quickly reveals weaknesses that would cause field failures. Moreover, HALT stresses the item to failure in order to assess design robustness.

HALT is not intended to demonstrate that the product will function properly at a specified stress level. It is intended to determine weaknesses so that they can be eliminated from the design. In the HALT process, the functional limits are explored. Failure modes are eliminated whenever feasible in order to expand the limits, and thus improve reliability and robustness. The objective is to increase the margin between the field environment and the operating / destruct limits of the product; generally, the larger the margin, the more robust the product and subsequently, the higher the reliability.

7.2.1 Approach. A Step Stress approach is used to determine, and expand, the operating and destruct limits of the product; the operating limit being the level (temperature, vibration, voltage, etc.) beyond which the product will not operate properly and the destruct limit being the level beyond which the product will undergo permanent damage. The idea of the Step Stress approach is to progressively increase the stress, which can be induced by thermal dwells, rapid temperature transitions, vibration, voltage, power cycling, etc., until a limit is discovered. At this point, a failure analysis is performed. Once the failure mode is known, corrective action can be taken as appropriate. This is repeated until the highest possible limits are found, which, in turn, will provide the highest possible operating and destruct margins and ultimately, the highest possible product reliability.

7.2.2 Failure Analysis. Fault detection is an essential part of HALT. Once a defect/weakness has transitioned from a latent state to a detectable state, there needs to be a way to detect that the fault has occurred. Functional testing ensures that all parts of the system are working properly. The functional test should be adequate enough to determine the performance of the system and the occurrence of multiple types of failure modes. During the test design, engineers exercise the major functions of the system with a feedback measurement of performance of the functions. The goal of the functional test is to achieve 100% coverage, or as complete test coverage as is possible.

Once the failure has been detected, Root-Cause Analysis (RCA) becomes an integral part of the HALT process. The objective of RCA is to determine the origin /root cause

of the underlying flaw or damage once it has transitioned from a latent state to a detectable state. This can be accomplished by examining the construction, manufacturing, packaging process or any progression beyond design and prototyping. In the case of field returns, field conditions under which the failure occurred may be simulated. These conditions might include temperature, vibration, voltage, frequency, humidity and any other relevant conditions. This approach is invaluable when assessing failure in fielded military products and acts as a cost effective tool that provides a qualitative understanding of the failure evolution in the product. The RCA process should be documented with each failure mode, the exact cause of the failure or the suspected cause, if uncertain and should include the results of a failure analysis with pictures of damage at the flawed site.

7.2.3 Corrective Action Verification. A corrective action plan is developed following the understanding of the failure mode through the RCA process. If the corrective action is easy to do and is a commonplace fix, then a RCA may not be needed. The corrective action “fixes” are summarized with a cause and effect report and accessed for cost vs. benefit tradeoffs. Based on this assessment a decision is made to implement the design changes or to leave the product unmodified. The engineering redesign decision process is defined and followed for all corrective actions. This should include a procedure and a reporting structure for review and decision-making authority to assess completeness and accuracy of the information reported.

Verification corrective action implementation is ensured by performing additional HALT testing subsequent to the corrective action process, as the product is redesigned. The design or process changes to the system are incorporated in the product samples subjected to the follow-on HALT with the goal being the assessment of the impact of the corrective action changes. The changes are investigated to determine if they improve or eliminate the discovered defects from the previous HALT, and if any other new problems have resulted from the changes.

7.2.4 Database Management. Due to the inherent historic nature of HALT testing and analysis, it is important to collect and maintain records regarding the weaknesses identified and the effective corrective actions. Logging the HALT data, so that it is easily indexed and searchable, helps to aid in the prevention of the reoccurrence of similar defects. The subsequent gains in ruggedization can help to decrease production costs by allowing more time compression during HALT screening.

7.2.5 Test Processes/Procedure. The HALT process advances through a series of exposures consisting of “Stress Sources” such as temperature variations, vibration, and electrical variations. The stress sources are modified in a “step-wise” approach from ambient to the extreme limits. The product is evaluated at each step. Failures are identified as “soft” failures that occur at extreme conditions, but recover at lesser stress levels, or as “hard” failures that permanently damage the item. These observations also establish the “Operating Limits” and the “Destruct Limits” of the product.

HALT consists of a minimum of four different tests. The first test is called the “Temperature Step Stress Test.” This test determines the operating and the destruct temperature limits of the product. The second test is a rapid thermal transition test, known as the “Thermal Transition Test”. The rapid thermal transition test is designed to determine the maximum rate of

temperature change that the product can withstand and bring out weaknesses from high transition temperature rates and low-cycle fatigue. The third test is the “Vibration Step Stress Test,” which determines the operating and destruct vibration limits. The final test is the “Combined Environment Stress Test.” This test determines the fatigue-based limits due to combined temperature and vibration loading. The combined environment is designed to facilitate the precipitation and discovery of fatigue weaknesses. During each test power cycling is performed periodically to expose additional failures or weaknesses. If a non-critical item experiences a failure and the failure mechanism is known, the item is bypassed or removed if it is too time consuming to fix, and the test is continued.

8. STRESS SCREENING METHODS

8.1 Highly Accelerated Stress Screening.

8.1.1 Overview. Highly Accelerated Stress Screening (HASS) is a quality control activity used to maintain reliability during the production process. It is a compressed form of HALT applied to the product to induce, detect, and fix weaknesses and flaws occurring during production. The screening uses the highest possible stresses determined in HALT, well beyond the qualification levels, in order to gain time compression. HASS may use the cross-over-effect technique by applying stresses which do not occur in the field to uncover flaws which might show up in the field due to other stresses. The screens must be of acceptable fatigue damage accumulation or lifetime degradation.

HALT is utilized to improve the design reliability by removing design weakness. The stress profiles for HASS can then be extracted from HALT. Therefore, HASS is generally not possible unless a comprehensive HALT has been performed as, without HALT, fundamental design limitations may restrict the acceptable stress levels to a great degree and could prevent the large accelerations that are possible with a very robust product. With the proper application of HALT, the design will have several, if not many, of the required lifetimes built into it and so an inconsequential portion of the life would be removed during the HASS analysis. The goal is to determine how much life is left in the system after HASS and not how much has been removed. Since the screening has to be performed on every part, proof of safety to ship the product after repeated HASS as well as effectiveness is essential.

HASS can be performed at many levels within a system. When dealing with components HASS may be carried out on components that are not mature, susceptible to damage or experience new operating conditions. HASS can also be utilized for subassemblies such as power supplies, hard drives, servo motors, communication radios, engines, etc. Assemblies and complete systems can also benefit from HASS such as avionics assemblies and unmanned ground and aerial vehicle systems. Another immense advantage of HASS is the ability to provide a cost effective approach to induce multi-axis vibration conditions on the product. This can be a reasonable alternative to single axis electrodynamic shakers.

8.1.2 Approach. The typical HASS analysis is a closed loop six step process consisting of at least: Precipitation, Detection, Failure Analysis, Corrective Action, Corrective Action Verification and Database Maintenance.

8.1.3 Precipitation. The objective of precipitation step is to precipitate latent defects, weaknesses and/or flaw sets in the production process that may, or may not, be uncovered in conventional qualification methods. Typically these defects evolve during the production process, which means that HALT does not uncover them.

8.1.4 Detection. Detection can be achieved via observation of abnormalities that exist in the product, either electrically, visually, functionally or by any other means. An abnormality may be intermittent in nature and may only be observable under particular conditions such as low temperature and/or low-level impact vibration. Some defects are not observable under full

screening levels of excitation even when the screen is within the operational limits of the equipment. Therefore, high stress coverage in HASS testing of the product is very critical.

8.1.5 Failure Analysis. The objective of RCA (Root-Cause Analysis) is to determine the origin /root cause of the underlying flaw or damage once it has transitioned from a latent state to a detectable state. This can be accomplished by examining the construction, manufacturing, packaging process or any progression beyond design and prototyping. In the case of field returns, field conditions under which the failure occurred may be simulated. These conditions might include temperature, vibration, voltage, frequency, humidity and any other relevant conditions. This approach is invaluable when assessing failure in fielded military products and acts as a cost effective tool that provides a qualitative understanding of the failure evolution in the product.

8.1.6 Corrective Action Verification. Corrective Action is the necessary means of implementing a change intended to eliminate the source of the flaw in future production. The objective of Corrective Action Verification step is to verify that through corrective actions defects and failures are eliminated in future product. Verification is achieved by repeating the conditions that caused a failure and verifying it is no longer present. A closed loop failure analysis and corrective action is necessary to ensure reliability improvement. Means of corrective action analysis and verification are discussed in Section 13.

8.1.7 Database Management. It is important to collect all of the data from the HASS in terms of manufacturing and processing flaws as well as implemented corrective actions so that a reoccurrence of the same defects can be prevented. Database management provides for an adequate comprehensive screening program.

8.2 Environmental Stress Screening.

8.2.1 Overview. ESS, like HASS, is a quality control activity used to maintain reliability during the production process. For more information see Section 12.2.1.

9. PHYSICS OF FAILURE

Physics of Failure (PoF) analyses provide a science-based approach to reliability that utilizes modeling and simulation to design-in reliability. The analyses use computer-aided design tools to model the root causes of failures such as fatigue, fracture, wear and corrosion. The basic approach involves the following:

- Identifying potential failure mechanisms (chemical, electrical, physical, mechanical, structural or thermal processes leading to failures); failure sites; and failure modes even before formal testing is complete.
- Identifying the appropriate failure models and their input parameters, such as material characteristics, damage properties, manufacturing flaw and defects, etc.
- Determining where variability exists with respect to each design parameter.
- Computing the effective reliability function.
- Accepting the current design or proposed design with new corrective action, if the estimated reliability exceeds the goal over the simulated time period.
- Proactively incorporating reliability into the design process by establishing a scientific basis for evaluating new materials, structures, and electronics technologies.
- Using generic failure models, where appropriate, that are as effective for new materials and structures as they are for existing designs.
- Encouraging innovative, cost-effective design through the use of realistic reliability assessment.

PoF analyses can be used to address long-term wear-out issues due to random vibration, thermal overstress or repetitive shock. Computer-Aided Design (CAD) tools have been developed to address various failure mechanisms and sites. Examples of failure mechanisms include metal fractures on various vehicle components or fatigue cracking of electronic solder joints.

The PoF analysis methods support contractors, PMs and engineers in all stages of acquisition from design, to T&E and fielded systems. In the design stage, system level dynamics models, component finite element models and fatigue-life models are used to reveal the underlying physics of the hardware in its mission environment. Outputs of these analyses include forces acting on a system, displacements of components, accelerations, stress levels, weak points in the design and component life. This information is used during the design process to make design changes early in the acquisition process when it is easier and more cost effective.

Design decisions and corrective actions made early in the acquisition phase lead to improved efficiency and effectiveness of the test and evaluation (T&E) process. The intent is to make fixes prior to T&E which will reduce test time and cost, allow more information to be obtained from test, and improve test focus. PoF analyses can be conducted for failures occurring during test to better understand the underlying physics of the problem and identify the root cause of failures which leads to better fixes for problems discovered, reduced test-fix-test iterations and reduced decision risk. The same analyses and benefits mentioned above can be applied to systems which are exhibiting failures in the field.

9.1 Mechanical PoF Approach. Mechanical PoF focuses on identifying root causes of failure including fatigue, fracture, wear, and corrosion prior to physical testing in an effort to mitigate potential failure mechanisms, yielding a more robust design for vehicle systems and other mechanically oriented assets. Numerous Computer Aided Design (CAD) and Computer Aided Engineering (CAE) tools have been developed to enable more accurate and rapid solutions to complex system failure analysis. Typical benefits of Mechanical PoF include designed-in reliability, a reduction in time-consuming and expensive testing, increased reliability of the fielded design, and decreased Operations and Support (O&S) costs. Figure 8 shows the major elements of the PoF approach to reliability.

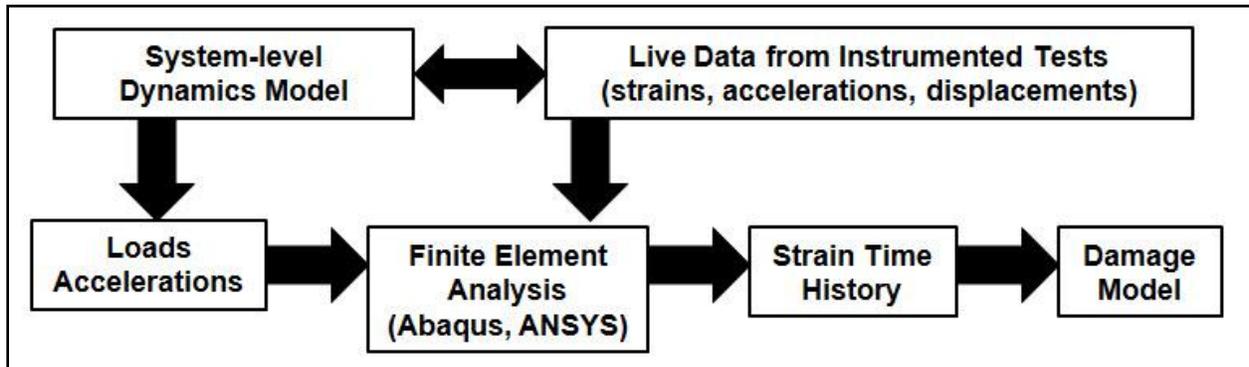


Figure 8. Mechanical PoF overview.

9.1.1 The Dynamics Modeling Process. Validated dynamics models can be used to supplement testing and extrapolate test procedures beyond typical safety limits. Model simulations can lower costs to Project Managers (PMs) by limiting required physical testing. As with most attempts at replicating operational conditions many assumptions and generalizations are often necessary to simplify the model. Inputs to dynamics models include bodies (components), hard points and joints, and action forces. The bodies are represented using CAD models and must include component mass, inertia values, and center of gravity locations. Hard points control the location and orientation of components in space, while joints dictate the connections and constraints between bodies, limiting the degrees of freedom. Typical forcing functions include Original Equipment Manufacturer (OEM) specific data and environmental usage data.

The dynamic modeling effort can require long developmental lead times and is heavily dependent on testing for validation. However, the validated model can provide a wide variety of data, including loading, acceleration and component displacement, with very minimal lead time. Load, acceleration, velocity, and displacement vectors along with component orientations can all be extracted from dynamics models. Output values from new models can be compared to corresponding test data for validation, while output values from mature models can be directly compared to component ratings to evaluate component fidelity.

9.1.2 Finite Element Method. A broad range of engineering analyses can be conducted using the Finite Element Method (FEM). These analyses typically address systems at the component level, but can be extended to full system models. FEM is a numerical analysis

technique where a geometric representation of a component or assembly is discretized into more basic shapes known as finite elements. The FEM, an accepted practice in industry, can be applied to obtain solutions to static/quasi-static stress analysis, dynamic load, frequency response (modal) analysis, thermal and heat transfer, fluid flow (computational fluid dynamics), and multi-physics (thermal and structural) problems. The list of software packages with some type of finite element analysis capability is expansive. The best software packages are validated against a wide variety of benchmarks, causing some to be considerably more trusted and versatile.

The FEM is completed in three steps: preprocessing, processing, and postprocessing. Finite element models require information related to geometric dimensions, material properties, boundary conditions, and external load vectors which are not always readily available. Many times assumptions and idealizations are necessary to account for information that cannot be obtained quickly and cost efficiently from a dynamics model or testing. Analysts must be proficient at assessing the validity of any assumptions made as every model with the essential constituents will provide an output. The accuracy of the model is entirely dependent on the validity of the inputs. Developing the finite element mesh, or the representation of the component or assembly using finite elements, is a critical part of preprocessing as results can be highly mesh sensitive. Finite element models should always be checked for convergence with regards to mesh refinement. The development of a finite element model should be an iterative process starting with a basic model and systematically adding higher levels of detail. There are various solver types for different problems and software packages that can be used to complete the processing phase of the FEM.

As with dynamics models, finite element models are deterministic and do not account for the variability that exists in the actual operating environment. The effectiveness of a model is dictated by the ability of the analyst to interpret and convey the results. This alludes to the fact that even though preprocessing is a time consuming and thought provoking process, post processing cannot be neglected or the benefits of the model will be diminished. The FEM provides a way to directly compare different products or design revisions under the same load conditions at a low cost. The primary utility of FEM is the capability of mapping inputs or measurements to those at critical locations with a component. Depending on the type of finite element analysis conducted, results may indicate the existence of overstress conditions due to stress concentrations, inadequate design, excitation at component resonance frequencies, etc. In addition, with the application of further analysis techniques, fatigue scenarios can be investigated.

9.1.3 Fatigue and Fracture. Fatigue is the reduction in strength or failure of a component due to cyclic stress from bending, axial loading, thermal loading, vibration, etc. The maximum stress values are lower than the Ultimate Tensile Strength (UTS) of the material, and often times are lower than the material's yield strength, and yet the cyclic nature of the loading eventually results in a failure. Fatigue can be exacerbated by stress concentrations including holes, notches, changes in thickness, and other abrupt changes in shape or cross-sectional area. If strain or loading is monitored at critical locations, Miner's Rule can be applied to predict the remaining life of a component under variable mean and amplitude loading. Miner's Rule states that load cycles act together linearly and damage accumulates consuming the fatigue life. Other

similar models attempt to address known deficiencies of Miner's formulation such as load sequence, nonlinearity, and multiaxiality. A third set of models that track crack propagation can be useful in predicting component life.

The application of Miner's Rule is facilitated using a cycle counting technique. Rainflow cycle counting, an efficient way of evaluating fatigue cycles for complex time histories resulting from variable amplitude loading, is the most commonly applied. Rainflow cycle counting involves reducing the time series data to a sequence of peaks and valleys arranged to begin with the absolute maximum. The signal is then treated as if it is filled with water and drained starting at the lowest valley, measuring total and mean depth drained until the entire signal has been completed. The fatigue damage for each cycle is calculated and then the cumulative fatigue damage is estimated using Miner's Rule.

Models also exist to convert the outputs of testing, dynamics models, and finite element models to life predictions. However, these models require extensive knowledge of material properties including the fatigue strength coefficient and exponent, and the fatigue ductility coefficient and exponent. Unfortunately these values are not typically available for less common or specialty materials. Methods for generating life predictions based on the material elastic modulus, yield stress, and ultimate stress are available. Phenomenological or statistics based models, which monitor and accumulate data that can be correlated to usage of individual components are also prevalent.

9.1.4 Testing. Within the Mechanical PoF process, testing is generally instrumented with the intent of acquiring specific physical data about a component or area of concern. Finite Element Analysis (FEA) used in conjunction with dynamics model outputs and general engineering judgment can identify "hot spot" locations for failures where instrumentation will be most beneficial. Typical measurements include, but are not limited to, strain, displacement, pressure, temperature, acceleration, vehicle speed, and vehicle motion (roll, pitch, yaw).

Test data is the primary source of information used to build and improve models and provide verification and validation. This information becomes even more important when manufacturer data is inaccessible. Modeling and Simulation (M&S) techniques are implemented to improve test efficiency regarding cost and schedule through the identification and resolution of failure mechanisms prior to testing. However, it is important to recognize that testing is an essential element of the PoF approach to reliability.

Testing cannot be entirely replaced, but rather is complemented by M&S. Testing complements modeling efforts by providing data for characterization, physical measurements critical for CAD model development, experimental modal analysis, dynamic tests vital for model inputs, and information regarding material properties. Physical testing can also have significant limitations, which can oftentimes be mitigated through the development and validation of analytical models. Measurements that are difficult to collect or that may be heavily operator dependent can be derived via modeling techniques. Test data that is limited to specific configurations (i.e. weight, center of gravity, test components, etc.) which can be negated or invalidated by modifications can be addressed via dynamic model efforts, which can be more easily adapted with configuration changes.

9.2 Electronic PoF Approach. An electronic PoF analysis typically consists of a thermal analysis (system-level and/or board-level), Circuit Card Assembly (CCA) thermal overstress assessment, CCA shock response analysis, CCA shock response assessment, CCA modal analysis, CCA random vibration response analysis, CCA thermal and vibration fatigue life assessments, and a CCA thermal plated-through hole (PTH) fatigue analysis. The system-level thermal analysis determines the temperature of the internal air and the chassis walls. It provides boundary information for the CCA thermal analysis. The CCA thermal analysis determines the steady-state temperatures of all components based on the temperatures at the CCA boundaries and the power dissipated by each component when the system is energized. Each steady-state component temperature is compared to its manufacturer's rated temperature during the thermal overstress assessment. The CCA shock response determines the board displacement and strain due to a given shock pulse. During the CCA shock survivability assessment, the computed board displacement and strain are compared to an empirically-based maximum allowable out-of-plane displacement and an acceptable board strain, respectively. The natural frequencies of a CCA are determined by the modal analysis. The CCA random vibration response analysis determines the displacement and curvature of a CCA due to random vibration loading. Based on input from the random vibration analysis and transportation/usage profile(s), the CCA vibration fatigue life assessment estimates the fatigue life of all component solder joints and leads on each CCA. The CCA thermal-fatigue life assessment determines each component's solder-joint life based on the number, magnitude, and duration of the thermal cycles (i.e., change in temperature due to powering on / powering down the equipment, change in temperature due to daily outside ambient temperature changes, etc.). The combined CCA thermal and vibration fatigue assessment predicts the fatigue life of all component solder joints and leads based on the cumulative damage due to vibration loading and thermal cycling. Finally, the CCA PTH fatigue analysis provides a life estimate of a PTH barrel in the CCA substrates based on the worst-case PTH geometry and the number, magnitude, and duration of the thermal cycles.

9.2.1 Operational Environment. It is very important to accurately model the environment in which the equipment will be operating. The environment is broken down into five parts within the circuit card assemblies' life cycle: Manufacture/Maintenance, Shipping/Handling, ESS/HASS, Transportation, and Operation/Mission Usage. Each produces different exposure levels and durations. The Manufacture/Maintenance, Shipping/Handling, and Environmental Stress Screening stages include all the stress cycles that the CCA experiences while being manufactured, handled in the factory, and screened for weak components. The Transportation stage includes the transportation of the circuit card assemblies from the factory to the field, where they are permanently installed in the end-use vehicle. The Operation/Mission Usage stage includes all damage accumulated due to operating the equipment in the field and is typically where most damage occurs.

The operation/mission usage is generally described in the Operation Mode Summary/Mission Profile (OMS/MP). The OMS/MP will provide annual operating time under vibration and annual number of equipment on/off cycles. The values in this table would be selected to most accurately estimate the vibration exposure levels on the CCAs being analyzed. The exposure levels can be evaluated for both move and idle operations.

Shock exposure levels are generally based on the Air Drop values given by the manufacturer, and the functional shock and crash values given in MIL-STD-810F.

9.2.2 Software. All analyses can be performed using commercially-available software. Examples include MathCAD (general purpose equation solver/plotter), ANSYS ICEPAK to conduct thermal analysis of the electronic chassis, MSC.Patran/Nastran (commercially-available general purpose FEA packages), macros written in Microsoft Excel 2003, and the University of Maryland's CalcePWA software.

9.2.3 Modeling the CCA. The first step in the electronic PoF process is to develop a detailed model of the CCA. In order to do this engineering drawings and associated parts lists and part information are necessary. CCA dimensions and board materials are also required. Printed Wiring Board (PWB) drawings that include overall dimensions, drill plan (including plated through hole/via sizes, locations, plating thickness, plating material, fill, etc.), and layer information (number of layers, layer thickness, total thickness, dielectric layer material, percentage of copper on each layer, etc.) are also needed. More detailed information allows for a much more accurate model of the CCA.

9.2.4 Modal and Random Vibration Response Analysis. CCA modal and random vibration response analyses are performed on each board to determine its first three natural frequencies and maximum displacement under the random vibration loading as specified for the analysis. The analysis results are used as inputs to shock and vibration fatigue life assessments. Lower dynamic displacements, which generally result from higher natural frequencies, are more desirable than higher displacements. Also computed is the random vibration dynamic displacement.

9.2.5 Thermal Overstress Analysis. Temperature is based on the individual power dissipations of the components on the CCA and the cooling performance of the system. Temperature on the CCAs will typically be highest in the area where components with highest power usage are located. The board temperature distribution is obtained from thermal analysis or test measurements. Junction temperature of each of the component is calculated or measured and compared to the manufacturers rated temperature.

9.2.6 Shock Response and Survivability Assessment. A CCA shock response analysis is performed on each board to determine its displacement and maximum strain due to the shock pulses. The CCA shock survivability assessment compares the maximum displacement and strain to an empirically-based maximum allowable out-of-plane displacement and acceptable board strain. The results are given in likelihood of failure.

9.2.7 Vibration Fatigue Life Assessment. The vibration fatigue assessment models provide an estimate of the fatigue life for CCA component interconnects (e.g., solder joints and component leads) based on input from the vibration analysis and Manufacture/Maintenance/Shipping/Handling/Stress Screening/Transportation/Operation/Mission profile(s). Failures occur due to stresses developed in the leads and solder-joints from the difference in relative curvature of the components and PWB and from in-plane accelerations acting on the components. Relative curvature and in-plane

accelerations continually change based on the input vibration (random and/or harmonic) load. The resulting stress fluctuations cause interconnect fatigue.

The results are given in terms of Damage Ratio (DR). The DR is the ratio of the actual number of cycles over a lifetime divided by the number of cycles that will cause failure. A DR greater than 1 indicates failure.

9.2.8 Thermal Fatigue Life Assessment. The thermal solder-joint fatigue assessment model provides an estimate of the fatigue life for CCA component interconnects (i.e., solder-joints). Failures occur due to Coefficient of Thermal Expansion (CTE) mismatch between the PWB and components. As the temperature goes up (or down), a component expands less than or greater than the PWB. The difference in expansion induces strain on the solder joints. The strain varies as temperature varies. Repeated, varying strain on the solder joints causes interconnect fatigue.

9.2.9 Combined Fatigue Life Assessment. The combined fatigue life assessment model provides an estimate of the fatigue life for CCA component interconnects (e.g., solder-joints and component leads) based on concurrent vibration (due to relative board curvature) and thermal loading (in-plane). The model utilizes Miner's rule of cumulative damage (i.e., accumulated damage is equal to the sum of the damage due to vibration and damage due to thermal cycling).

9.2.10 Design to Reduce Vibration/Shock Failures. As indicated above, circuit cards are susceptible to damage from vibration and shock environments. Vibration can lead to the following problems:

- Loosening of fasteners
- Wire chafing
- Touching and shorting of electronic parts
- Optical misalignment
- Material cracking or rupture
- Electrical noise
- Intermittent disconnecting of separable contacts
- Fretting wear of separable contacts
- Interconnect fatigue failures
- Shorting or fracture of parts due to dislodged particles or parts

There are four basic types of shock failures including the following:

- Fractures or permanent deformations due to high stresses;
- Loosening of bolts and supports from the high acceleration levels;
- Impact between adjacent CCAs due to high displacement; and
- Electrical malfunctions of the CCA components due to the component's internal structures deforming (may only malfunction during the shock load).

The following points address good design practices for the reduction of vibration/shock failures. The ideal situation is to use these guidelines to provide a better initial design, however these are also actions that can be taken if a PoF analysis identifies damage due to shock and vibration loads.

- Increase the first natural frequency of the circuit board, which will decrease the board displacement and curvature. In general, higher natural frequencies of CCAs result in lower displacements and a greater resistance to vibration loads.
- Increasing the natural frequencies can be accomplished by stiffening the CCA, decreasing the weight of the CCA, or by changing the way the CCA is supported in the electronic box.
- Supports desirable for vibration firmly attach the CCA to the electronic box. These supports reduce deflections, translations, and edge rotations. Firm supports increase the CCA natural frequencies.
- Adequately support the circuit card on four sides and the middle of the card. Generally, the more supports, the less board displacement and curvature although strategically placing the support can have the same effect. With the reduction of board curvature, the stress on the component body, leads and solder joints are reduced.
- In addition to CCA supports, rib stiffeners can be used to increase the natural frequencies. Select ribs that have a relatively high modulus of elasticity, such as steel, copper or brass. Ribs may be soldered, bolted, welded, or cemented to the PWB, and may be undercut to allow circuitry to pass beneath them.
- Place rib stiffeners so that the load is directed to a support, not a free edge of the board.
- Locate vibration or shock-sensitive components to areas of the board with less curvature, which is usually close to the supports.
- Separate the natural frequencies of the electronic assembly and the CCA. When the CCA has two times the natural frequency of the assembly, or vice versa, severe dynamic coupling effects are reduced. This is called the octave rule because the natural frequencies are separated by one octave.
- Include shock isolators for the electronic assembly if relatively large shock pulses are expected (greater than 50 Gs), especially if circuit cards are subjected to repeated gunfire shock. Shock isolators reduce the magnitude of the shock transmitted, which protects the CCA from excessive displacements and failure.
- The shock isolators must be designed for vibration as well as shock. Unfortunately, isolators that are good for shock are generally not effective for vibration, and vice versa.
- Design the shock isolators for anticipated shocks. If the isolators are designed incorrectly, then shock amplification can occur. The ratio of the first natural frequency of the CCA and the natural frequency of the shock pulse must be known to determine the potential shock amplification.

The following points are rules of thumb for vibration and shock-related failures. Again, paying attention to these can lead to a better initial design. However, if a PoF analysis

identifies damage due to shock and vibration environments, the following list can provide insight to increasing fatigue life.

- Larger components are usually more sensitive to vibration/shock loading. The curvature under the component is greater because of the larger component length. Package length in the direction of bending is a critical parameter.
- Leaded surface-mounted components are more robust for vibrational stress than leadless components such as ball-grid array packages or leadless ceramic chip carriers.
- Very stiff packages and stiff leads reduce the solder-joint fatigue life.
- Axial-leaded components are less sensitive to shock and vibration stress.
- Shock and vibration failures in ball-grid array packages are usually at the corner solder joints.
- Ceramic leadless chip capacitors and tantalum-leaded capacitors are more sensitive to shock loading than other types of capacitors. To a lesser extent, ceramic multi-layer chip resistors, quad flat packs, and DIPs are sensitive to shock loading.
- For shock and vibration loading, the components or leads usually fail rather than the solder joints.
- Components (DIPS or quad gullwing packages) mounted in sockets are not appropriate for circuit cards that experience shock loads. Gluing the components into the sockets would help but would eliminate some benefit from the sockets.

9.2.11 Design to Reduce Temperature Cycling Failures. Probably the most significant aspect of temperature is not high or low temperature extremes, but the change of temperature (i.e., temperature cycling). Electronics are composed of many different materials that have wide ranges of coefficients of thermal expansion (CTE). These wide ranges of CTE along with extreme changes in temperature result in significant thermo-mechanical strains. Such changes in temperature may occur during manufacturing (e.g., vapor depositions and soldering operations), external environmental changes, and normal power cycling. Specific failure mechanisms accelerated by temperature cycling include:

- Solder-joint fatigue
- Plated-through hole or via barrel fatigue
- Plated-through hole or via barrel buckling
- Delaminations between the layers of the composite
- Delaminations between the composite and the metallization

There are several approaches to dealing with temperature in electronics. A list of mitigation activities to be done during the design process or as a result of PoF analysis includes the following:

- Reduce temperature cycle range. The selection of the heat transfer technology and equipment can be used to constrain electronic temperatures to reduce the electronic temperature cycle range.

- Reduce the temperature cycle by placing the components dissipating the most power closer to the heat sink (or thermal path away from circuit card).
- Avoid rapid changes in temperature.
- Match the CTE of the electronic components and the circuit board to reduce stress on leads and solder joints, and increase fatigue life.
- Use underfill (epoxy material that goes under a component) for components with a large CTE mismatch with the circuit board. Ensure the underfill material's CTE is not large in the direction perpendicular to the component, or the underfill may induce stress in the leads.
- Only use underfill as a last resort, because it complicates the manufacturing and repair processes.

The following points are rules of thumb for temperature cycling-related failures. These often lead to recommendations for component/package changes as a result of thermal PoF analysis.

- Leadless components are more sensitive than leaded components to temperature cycling. The leads help reduce the stress on the solder.
- The more compliant the leads, the less stress in the solder.
- Large packages are more susceptible to thermal cycling (the larger distance from the neutral point) than smaller packages.
- Outer leads/solder joints have the most stress (largest distance from the neutral point) and will fail first.
- Avoid the use of ceramic leadless chip caps on FR-4 (fiberglass epoxy) boards.
- CTE of plastic epoxy packages vary, because there are many different epoxy materials, and die size can reduce the CTE (especially when the package size approaches the die size).
- Ball-grid Array (BGA) package CTE varies over the package length, because the area under the die (die shadow) is constrained by the die material (CTE of silicon is lower than epoxy).
- For BGAs, the die shadow solder balls may fail before the outer solder balls.
- The more solder used, the longer it takes for the crack to propagate through to cause a failure.

9.2.12 Design to Reduce Thermal Overstress Failures. Temperature plays an important role in the reliability and performance of electronics and CCAs. Temperature influences reaction rates, changes material behavior, and may degrade operational characteristics of circuits. The selection of the heat transfer technology and equipment can be used to constrain electronic temperatures below the formation temperatures and to reduce the electronic temperature cycle range. Thermal analysis can then be performed to determine the effectiveness of this technology and equipment. The goals of heat transfer include removing the heat dissipated by the components, constraining component temperatures below the rated operational values, and minimizing thermal gradients between components. To control component temperatures, the heat must be transferred from the component to a heat sink. Typical heat transfer ranges from $0.2\text{W}/\text{cm}^2$ to $20\text{W}/\text{cm}^2$. Other factors that influence the heat transfer technology and equipment include cost, weight, location, accessibility, maintainability, fan noise

level limits, and power consumption of thermal control mechanisms. These factors should be considered when selecting the heat transfer technology and equipment.

The following points address good thermal design practices/recommendations coming out of a PoF thermal analysis.

- Determine actual power being dissipated for each component from the electrical simulation. Rated powers in datasheets are no indication of actual power.
- Ensure all components are below their rated temperature (some component types may work over their rated temperature, but there is no guarantee that all components of that type will operate correctly over their rated temperature). Changes in manufacturing or assembly (unknown to the purchaser) may cause the component to operate differently in high temperatures.
- Determine if the rated temperature in manufacturer's datasheets is for the die or package (there is no standard). If there is uncertainty about whether the rated temperature is for the die or package, assume it is for the die.
- Place components dissipating the most power closer to the heat sink (or thermal path away from circuit card).
- Obtain junction-to-case thermal resistance values from component manufacturers, because this affects die temperature.
- Use thermally conductive material under components to increase heat flow out of the components.

9.3 Summary. Physics of Failure can provide significant benefits regarding the reliability of equipment at all stages of the acquisition process. PoF can assist in assessing reliability during source selection, identify potential failure locations early in the design process, determine the root cause of failure during testing, improve the accuracy of ALT, and provide assessments of upgrades and field kits. Applying mechanical PoF in the design phase results in the discovery of potential reliability and durability problems at a more opportune and cost effective time for corrective action. PoF provides testers, evaluators, and program managers with a tool to improve the efficiency and focus of Test and Evaluation (T&E) by identifying failure modes and optimum sensor locations prior to testing. This enables the value of each test to be maximized. It can be used to supplement testing when scheduling does not permit sufficient time for all the desired tests or the test asset availability is limited. Ultimately, PoF reveals the underlying physics of the hardware in its mission environment resulting in an increase of knowledge which will directly benefit the consumer, lower life-cycle costs, improve performance, and increase reliability.

10. SOFTWARE-IN-SYSTEMS RELIABILITY

10.1 Reliability Block Diagrams and Reliability Allocation. Most of the work required for incorporating software into a system Reliability Block Diagram is in predicting the failure rate and subsequent reliability of each software component. Once that has been accomplished, it is a relatively simple task to multiply the reliability allocation of each hardware component by its associated software component reliability. Thus when software is part of a system, it can be considered to be in series with the associated hardware in terms of an overall reliability assessment.

The allocation of software reliability involves the assignment of quantified reliability goals to individual computer software configuration items (CSCI) based on the top-level reliability requirements of the system software. It is critical that the allocation of software reliability requirements be performed as early as possible in the program so that achieved reliability levels can be assessed against their allocations for compliance. The basic techniques for performing software reliability allocation are:

- Sequential Execution (equal allocation applied to sequential software CSCIs)
- Concurrent Execution (equal allocation applied to concurrent software CSCIs)
- Operational Profile (allocations are based on mission or operational profiles)
- Complexity (allocations are based on software complexity factors)
- Operational Criticality (allocations are based on the mission or operational criticality factors)

Allocation of system-level reliability requirements to software elements makes sense only at the software system or CSCI level. Software reliability requirements may only be stated for the highest indented level of software, or they may be buried within an overall system-level requirement that includes elements of both software and hardware reliability. In either case, software reliability requirements should ultimately be decomposed into lower level computer software configuration and CSCI reliability requirements in order to drive software reliability design at these lower levels of software indented. A different approach is needed to flow down those allocations to lower levels of software. For each mode in a software system's operation, different modules (CSCIs) will be executing, with each mode having its own operating time element associated with it. A basic "model", should be constructed to illustrate which modules will be operational during each system operational mode. The duration of each operational mode should also be identified.

The software reliability model should include the number of lines of source code (SLOC) that is expected within each module. This data, along with other relevant information pertaining to the available software development resources (i.e., number of personnel, computing facilities, test facilities, etc.), is subsequently used to define the initial failure intensity predictions for each of the defined software modules.

Once the reliability requirements are allocated, it is necessary to track and project whether these requirements are or can be met at the present time, or sometime in the future. This

is accomplished by collecting and analyzing data to identify the selection of a suitable reliability prediction and/or estimation model.

10.2 Software Reliability Growth Testing. Software failures arise from a population of software faults. A software fault (often called a "bug") is a missing, extra, or defective line of code that has caused, or can potentially cause, a failure. Every time a fault occurs during execution, a failure does not necessarily result; it depends on the machine state (values of intermediate variables).

The failure rate of a piece of software is a function of the number and location of faults in the code, how fast the program is being executed, and the operational profile. While most repair activity is imperfect, the hoped-for and generally-observed result is that the times-between-failure tend to grow longer and longer as the process of testing and fault correction goes on. A software reliability growth model mathematically summarizes a set of assumptions about the phenomenon of software failure. The following models, from Rome Laboratory report RL-TR-92-15 "Reliability Techniques for Combined Hardware and Software Systems," provide a general form for the failure rate as a function of time and contain parameters that are determined either by prediction or estimation. These models can be used to estimate the reliability of initially released software, along with the reliability growth which can be expected during debugging.

- Initial Software Failure Rate
- Software Reliability Growth

Formal reliability growth testing for software, similar to that for hardware, is performed to measure the current reliability, identify and eliminate the root cause of software faults and forecast future software reliability. Software reliability growth testing should always be performed under the same operational profiles as those expected in the field in order to be effective.

There are, literally, hundreds of software reliability growth, prediction and estimation models available. The accurate and effective measurement and projection of reliability growth requires the use of an appropriate mathematical model that describes the variation of software reliability behavior over time. Parameters for these growth models can be obtained either from Design for Reliability analyses and testing performed during the time period that precedes formal reliability growth testing, or from estimations performed during the test. Some of the most common software reliability models include:

- General Exponential
- Musa Basic
- Musa Logarithmic
- Littlewood/Verrall
- Schneidewind
- Duane
- Brooks and Motley
- Yamada, Ohba & Osaki S-Shape

- Weibull
- Geometric
- Thompson & Chelson Bayesian
- Rome Laboratory (RL-TR-92-15)

With the number of potential models available, it is not easy to select which model may be most appropriate for a specific situation. Figure 9 attempts to provide some guidance on model selection based on the following constraints:

- Failure profiles (failure intensity trend)
- Maturity of software (what phase of its life cycle is the software in)
- Characteristics of software development (how are failure modes detected/mitigated)
- Characteristics of software test
- Existing metrics and data

If the plot of failure intensity vs. cumulative test time is showing an increase in failure intensity (negative reliability growth), then you need to make sure that the software is in an operational state, that only unique software failure modes are being counted, and that all time estimates are accurate. If these conditions are satisfied, it is likely that the software is still in the early stages of system development or test.

If the plot of failure intensity vs. cumulative test time is decreasing, you must still make sure that the software is being tested or used in an operational profile that is representative of how it will be used in the field, and that there have been no failures experienced for a reasonably significant period of time.

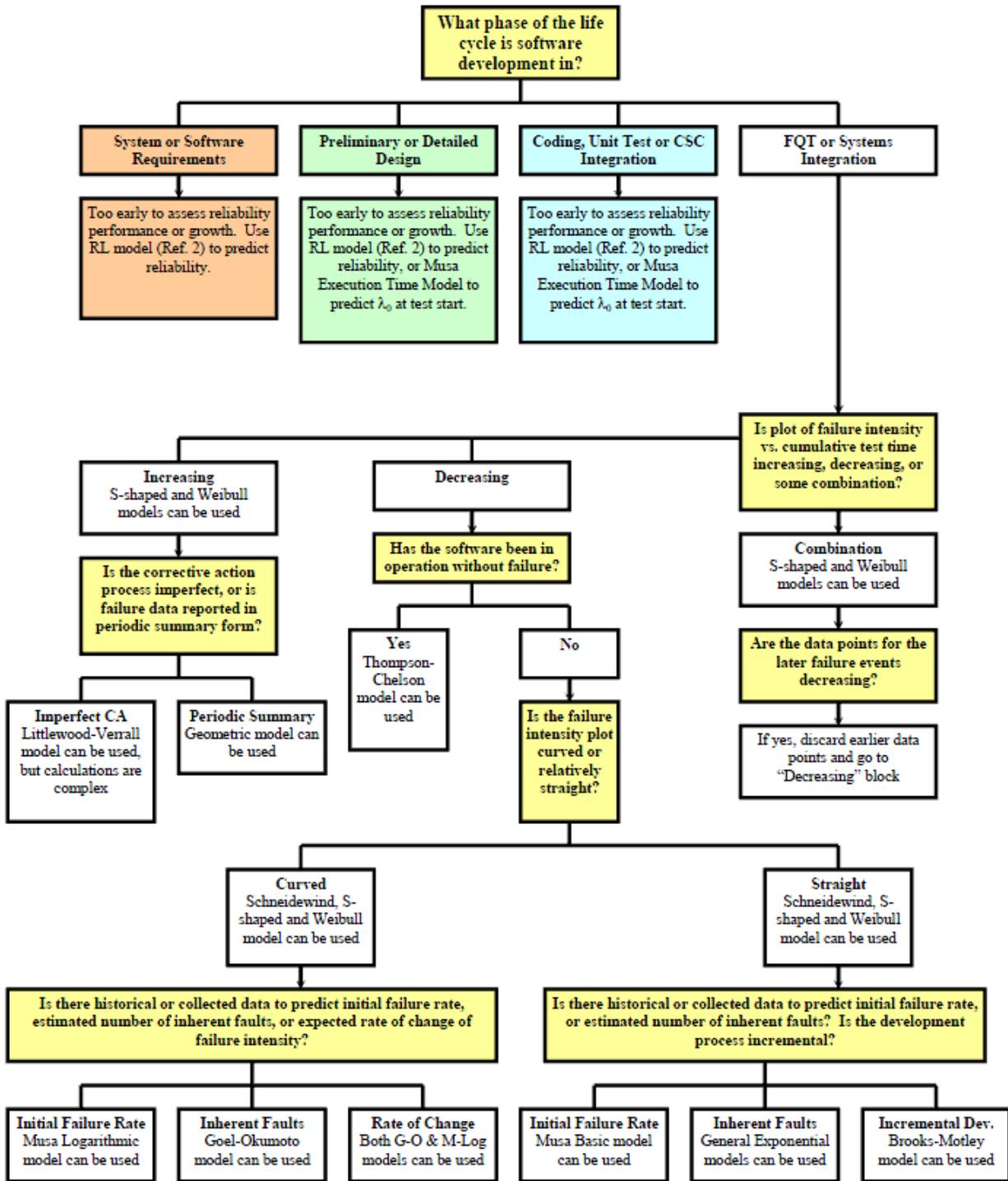


Figure 9. Selection of a Software Reliability Growth Model.

10.3 Software Reliability Testing. The purpose of this topic is to recognize that testing currently plays a critical role in the success of both large and small software projects, and will continue to do so in the foreseeable future (unless someone comes up with a foolproof, repeatable process for developing and integrating software that possesses perfect reliability (zero defects), in which case testing of software will become obsolete).

Figure 10 identifies several reasons why software testing needs to be performed. In all cases except one (reliability demonstration testing), the success of a test is measured by the number of defects that it detects (assuming that they are ultimately corrected, resulting in positive reliability growth), not by completion without failures.

Reason	Comments
Detect, expose and correct defects	Defects can be in code, requirements and/or design. Gives programmers information they can use to prevent future defects.
Demonstrate that requirements have been satisfied	The rationale for any test should be directly traceable to a customer requirement (whether explicit or implicit)
Assess whether the software is suitable to meet the customers' needs	Give management the information it needs to assess potential risks associated with the product
Calibrate performance	Measure processing speed, response time, resource consumption, throughput and efficiency
Measure reliability	Quantify the reliability of the software for the customer (reliability demonstration), or for internal improvements (reliability growth) prior to delivery to the customer
Ensure changes/modifications have not introduced new faults	Referred to as regression testing
Establish due diligence for protection against product liability litigation	May provide some level of protection against (justifiably or unjustifiably) dissatisfied customers

Figure 10. Reasons to Test Software.

10.4 Software FMECA. The probability of being able to guarantee that software will be error-free is virtually zero, primarily due to the fact that the two basic methods for demonstrating that software is correct, proof of program correctness and comprehensive testing, are cost and resource prohibitive, particularly with regard to highly complex software intensive systems. Potential software defects identified using analyses such as FMEA and FTA, or even precipitated during testing, do not always lend themselves to total elimination. In these cases, the software design must be changed to somehow tolerate the occurrence of a failure so as to reduce its risk and severity impact on overall system performance, reliability and safety.

In specifically addressing software FMECA, a general procedure is to:

- Break the software into logical components, such as functions or tasks
- Determine potential failure modes for each component (e.g., “software fails to respond” or “software responds with wrong value”)

- Using a failure mode table, use the failure modes to fill in the Software FMECA worksheet (Figure 11 below)
- Determine all possible causes for each failure mode (e.g. “logic omitted/implemented incorrectly”, “incorrect coding of algorithm”, “incorrect manipulation of data”, etc),
- Determine the effects of each failure mode at progressively higher levels (assume inputs to the software are good)
- Assign failure rates; occurrence, severity and detectability values; and calculate the Risk Priority Number (RPN)
- Identify all corrective actions (CAs) that should be, or have been, implemented, plus all open items

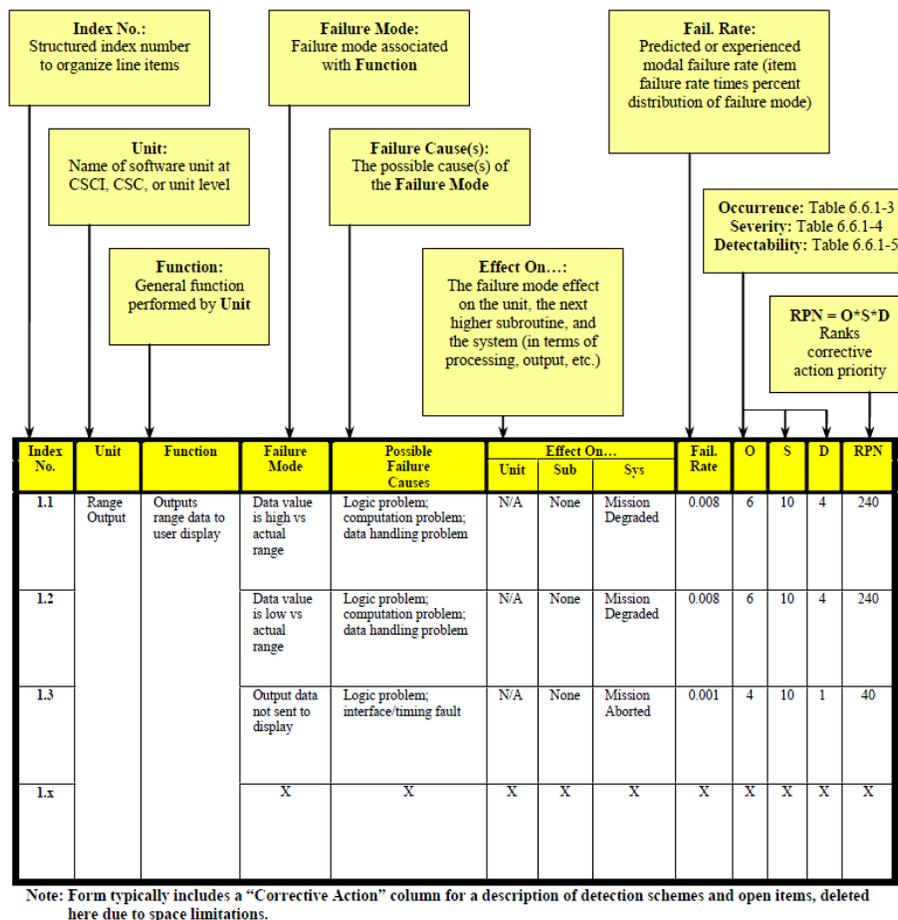


Figure 11. Sample Software FMECA Worksheet.

10.5 Fault Tree Analysis for Systems Containing Software. To be most effective, a system-level FTA must consider software, hardware, interfaces and human interactions. Top-level undesired events may be derived from:

- Engineering judgment based on what the system should ultimately not do
- Problems known from previous experience, or from historical “clue lists”
- Outputs of a FMEA – or a FMECA

- Information from a Preliminary Hazard Analysis

The basic steps for performing a FTA for software (same as for hardware) are as follows:

1. Definition of the problem
2. Analysis Approach
 - a. Identify the top-level event
 - b. Develop the fault tree
 - c. Analyze the fault tree
 - i. Delineate the minimum cut set
 - ii. Determine the reliability of the top-level event
 - iii. Review analysis output

An FTA that involves system software typically makes use of a specific clue list, where a “clue list” represents items that have historically caused problems (such as conditional “GO TO” statements in software), or are likely to be a problem (such as inadequately controlled boundary conditions). These lists typically evolve over a long period of time and are generally based on the experience of the analyst, the design team, or the testing organization. They may also be developed for hardware-related or human-machine related problems, but the concept is illustrated here based on potential software problems. Figure 12 which is derived from the Software System Safety Handbook provides a “clue list” for software representing several items that have been found to historically cause problems. It is not a “set” list, in that it should be tailored or appended based on the coding language and software architecture that is being used for a specific application.

a.	Ensure that all variables are properly defined, and data types are maintained throughout the program
b.	Ensure that, for maintainability, variables are properly defined and named
c.	Ensure that all safety-critical data variables and processes are identified
d.	Ensure that all code documentation (comments) is accurate and that CSCI/CSU headers reflect the correct processing and safety-criticality of the software
e.	Ensure that code and date modifications identified as a result of Software Trouble Report resolutions are made
f.	Ensure that processing loops have correct starting and stopping criteria (indices or conditions)
g.	Ensure that array subscripts do not go out of bounds
h.	Ensure that variables are correct in procedure call lines (number, type, size, order)
i.	Ensure that, for parameters passed in procedure call lines, Input-Only data is not altered, output data is set correctly, and arrays are properly handled
j.	Ensure that all mixed modes of operation are necessary, and clearly documented
k.	Ensure that self-modifying code does not exist
l.	Ensure that there is no extraneous or unexecutable code
m.	Ensure that local variables in different units do not share the same storage locations
n.	Ensure that expressions are not nested beyond 5 levels, and procedures/modules/subroutines are less than 25 lines of executable code
o.	Ensure that all logical expressions are used correctly
p.	Ensure that processing control is not transferred into the middle of a loop
q.	Ensure that equations are encoded properly, in accordance with specifications
r.	Ensure that exceptions are processed correctly. In particular, if the “ELSE” condition is not processed, will the results be satisfactory?
s.	Ensure that comparisons are made correctly
t.	Ensure that common blocks are declared properly for each routine they are used in
u.	Ensure that all variables are properly initialized before use

Figure 12. Potential "Clue List" for Software Problems.

11. SYSTEM AND SUB-SYSTEM LEVEL PROTOTYPING

11.1 Background. Prototyping is the process of creating a physical model of an intended design. The purpose of the prototype is to create a small number of systems or subsystems with the intent on testing the model before more costly expenditures are conducted in the production phase. The goal of system and sub-system level prototyping is to identify if the prototype will meet specifications set forth. This can be accomplished through a variety of ways to include, but not limited to the following:

- Design Verification Testing – Does the prototype meet the specifications and perform its mission within a certain confidence?
- Accelerated Life Testing – Have all possible failure modes that this system or sub-system will see during its life-cycle been identified?
- Interface Testing– Does the system perform to its specifications when integrated with other systems?

A prototype can be an exact replica or a scaled version of the intended design. A common method to analyze a design is the prototype, test, and analyze method shown in Figure 13. This is a cyclical process which continues until a robust design is created.

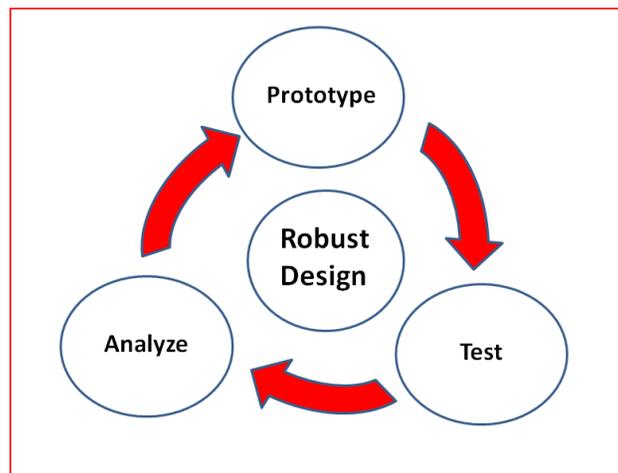


Figure 13. Robust Design Cycle.

11.2 Benefits of Prototyping Early in the Design Phase. Modeling and simulation are excellent tools for analysis early on in the design phase, but providing customers and engineers scale models of the system or sub-system can prove to be beneficial as well. These models can be used to create manufacturing and production procedures and can be used as marketing tools to potential customers. Physical models can often be used to identify human factors concerns or functional issues commonly missed with 3D CAD models.

Identifying failure modes and corrective actions of a prototype early on in the design phase can provide cost savings during the production phase and throughout the life cycle of the product. Also, bringing to light failure modes that may not be identified until late in the life

cycle and implementing corrective actions may prove to provide significant cost savings to both the manufacturer and the customer.

11.3 Rapid Prototyping. This process is intended to create models without creating expensive tooling and to hasten the time to market. Rapid prototypes can be created in hours with Stereolithography (SLA) or 3D Printing technologies rather than in days using costly procedures like Injection Molding, Casting, or CNC Machining. Rapid prototypes can be made with a variety of materials with mechanical properties similar to what was intended for design.

However there are drawbacks to the rapid prototyping process. The models are usually not exact representations, and may not have the same strength and toughness as the designed material. Additionally, the geometric tolerances for rapid prototypes are normally outside what can be achieved with traditional fabrication processes like CNC Machining and Injection Molding.

11.4 Design Verification Testing. Design Verification is conducted on a sample size of prototypes to determine confidence in functionality. The purpose of this test is to prove, with a certain level of confidence, that the system or sub-system will meet or exceed all intended specifications. This can be accomplished through instrumented testing where a system or sub-system is operated over its duty-cycle while reaching the maxima and minima of the specifications. This instrumented data is recorded and then is used to feed mathematical or physics based models. This testing can also be conducted on a pass/fail criterion where component failures are recorded.

11.5 Interface Testing. Interface testing is one of the most common forms of testing and is normally conducted early on in the design phase. An interface test is performed in order to determine if the systems or subsystems work as intended with other components in the system. This test can be as easy as a check for form and fit and as rigorous as testing whether the system performs as intended during integration.

12. TEST AND EVALUATION

12.1 Test and Evaluation. Test and Evaluation (T&E) is the process by which a system or a system component is compared against requirements and specifications through physical testing. The results are evaluated to assess progress of design, performance, supportability, etc. Developmental test and evaluation is an engineering tool used to reduce risk throughout the defense acquisition cycle. Operational test and evaluation is the actual or simulated employment, by typical users, of a system under realistic operational conditions.

12.2 Testing.

12.2.1 Environmental Stress Screening. Environmental Stress Screening (ESS) is utilized to expose a product to extreme environmental conditions in order to cause early failures due to design flaws or production problems. The intention is to perform this type of testing initially at low-indenture levels to understand how resilient components are to environmental effects. Some examples of environmental effects include solar loading, humidity, wind, extreme temperatures (cold and hot), and exposure to other elements such as acid rain, blowing sand, salt water, blowing dust etc. A variety of failure modes and design modifications arise out of environmental testing. Identification and mitigation of environmentally-induced failure modes is of paramount importance for ensuring product quality, especially when typical use conditions for an item may be severe. One of the most well-known environmental tests is the 85/85 temperature and humidity stress-test developed by Western Electric in the late 1960s. This test exposes devices to 85 degree Celsius temperatures and 85 percent relative humidity to study corrosion effects of metallic wire bonds. The pressure-cooker test method developed by Japanese integrated circuit manufacturers in the 1970s is another popular environmental stress test. It was utilized to evaluate moisture resistance and analyze corrosion kinetics of plastic encapsulated integrated circuits.

12.2.2 Accelerated Life Testing. Accelerated Life Testing consists of testing a product at high levels of stress in order to transform hidden or latent defects into detectable failures. The data that is captured under accelerated conditions is extrapolated, through a physically reasonable statistical model, to make inferences about the life distribution of the product under normal stress levels. There are a number of physical stresses that may be accelerated including moisture, elevated constant temperature, temperature cycling, fixed vibration, random vibration cycling, electrical power cycling, maximum output loading, etc. The intention of stressing products in this manner is to efficiently uncover the existence of any failure mechanisms, understand the extent to which they pose a problem, and develop a corrective action strategy to enhance the component's resiliency and reliability. There are a wealth of statistical procedures, test methodologies, and mathematical models available for accelerated life testing.

12.2.3 Design of Experiments. Design of Experiments (DoE) and the Analysis of Variance (ANOVA) techniques are economical and powerful methods for determining the statistically significant effects and interactions in multivariable situations. DoE may be utilized for optimizing product designs, as well as for addressing quality and reliability deficiencies. Within the DoE framework, the practitioner may explore the effects of a single variable or

analyze multiple variables. A multivariable analysis is often referred to as a “factorial experiment.” An example of how DoE would be used in a DoD context that is relevant to reliability engineering includes supplier selection for the use of COTS items, GFE, or other non-developmental devices that may be used in a given acquisition program. A common approach would be to test a sample of bearings, for instance, from each of four different vendors until they are run to failure. Using DoE, one can quantify the variation between samples and determine if the variation is statistically significant, or if perhaps it is only an artifact of the variations within the populations from which the samples were randomly drawn. Of course, the ultimate goal is to make an inference regarding the variation in product quality across vendors, as well as within the individual populations.

Factorial experiments may be extended to analyze two or more sources of variation. Leaks of O-ring seals within hydraulic systems, for example, can result from multiple factors, such as, excessive oil pressures, extreme temperatures, or installation error. DoE methods may be used to analyze these sources of variation, determine interactions that may occur between them, and identify the statistical significance thereof. There is a great deal of literature covering the subject, and a number of different DoE techniques have been developed.

The Taguchi Method is a popular approach that is tailored to the requirements of the engineering design. The method consists of three phases system design, parameter design, and tolerance design. The system design phase focuses on the material concept and determining the required performance, quality, and reliability characteristics. The parameter design stage focuses on refining parameter values to optimize the desired characteristics of the system relative to the sources of variation and the interactions between them. The final stage, tolerance design, highlights the effects of random variation, e.g., manufacturing and production processes, to determine if further design margin or optimization is needed. Of course, the value of reaching a given level of design margin is constantly assessed in terms of investment cost versus the current level safety, quality, performance, reliability etc. that has been achieved.

12.2.4 Reliability Qualification Testing. Reliability qualification testing is utilized to verify if a given product possesses advertised or established reliability requirements. This type of testing is particularly useful for checking the reliability of COTS items, GFE, and other non-developmental components. Reliability qualification testing is focused on the design of a product, and is also known as reliability demonstration, or design approval testing.

12.2.5 Reliability Production Testing. Reliability production testing is utilized for assurance that production deficiencies do not degrade reliability of an approved design of a product. Packaging processes, for instance, are a major source of manufacturer-induced reliability deficiencies for electronic components. In both qualification and production testing, units from the production line are randomly selected for testing. For both cases, binomial- and exponential-sequential test procedures offer an efficient method by which product reliability may be accepted, rejected, or verified.

12.3 Physics of Failure and Testing cooperation. Testers, Evaluators, and Program Managers are continually challenged with the question of obtaining the most value from each T&E exercise conducted. Physics of Failure (PoF) aids system evaluation by revealing the

underlying physics that explain system performance and helps identify root-causes of test and field failures. As such, PoF and Testing are two important aspects of reliability that go hand in hand to make the best use of time and money.

12.3.1 System Level Testing. System level testing is used to determine the subsystem's loading. This includes instrumentation of various locations with thermocouples, accelerometers, and/or strain gauges to gather temperature, vibration, shock, and stress information that is necessary for input into PoF models. System level test results are useful for determining load and acceleration profiles, characterizing acceleration data with Power Spectral Density (PSD) plots, and investigating thermal environment. Typically the data obtained in testing is used to provide accurate input information for PoF analyses.

12.3.2 Survey Testing. Survey testing is used to refine and verify analysis predictions. It is also used to determine the interaction of multiple assemblies and chassis. Survey testing includes vibration (modal), thermal, and shock analysis procedures.

12.3.2.1 Thermal Survey Testing. A thermal analysis predicts component temperatures and identifies components to monitor. Thermal survey testing measures actual component temperature using thermocouples, thermal imaging, or both. Infrared imaging provides a thermal map of the object being tested.

12.3.2.2 Modal Testing. Modal or Random Vibration analyses predict natural frequencies and identify locations of maximum deflection for accelerometer placement. Modal testing measures the actual natural frequencies of subsystems and chassis.

12.3.2.3 Shock Testing. Shock testing measures strain response of components such as a circuit card and the test determines the shock response of the components and the Shock Response Spectrum if testing at a sub-system level.

12.3.3 Component Analysis Testing.

12.3.3.1 Thermomechanical Testing. Thermomechanical testing is used to determine material properties such as Coefficient of Thermal Expansion and Modulus of Elasticity. The captured data is typically used to verify and refine the PoF modeling process.

12.3.3.2 Failure Analysis Testing. Failure analysis testing is used to verify the failure mechanism and root cause. It can be conducted through either non-destructive testing such as Scanning Acoustic Microscopy, Scanning Magnetic Microscopy, Fourier Transform Infrared Spectroscopy, Atomic Force Microscopy or through destructive test such as decapsulation or delidding. Failure analysis testing can determine component internal structure for advanced PoF and the results are used to recommend reliability improvements.

12.3.4 Reliability Enhancement Testing. Reliability Enhancement Testing (RET) is used to find failures in a product due to environmental stresses. RET is applied to determine upper and lower operating and destruction limits, the life of product or component, where and what failures could occur in materials, components, manufacturing, and design given there are no

defects, and the environmental stresses which cause failure. It also helps to correct failures before production begins and increase reliability to ensure that a product is robust. Thermal cycling, vibration testing, shock testing, HALT, and Highly Accelerated Stress Test (HAST), used for temperature, humidity, and pressure stress analysis, are all considered within the RET envelope.

13. CORRECTIVE ACTIONS AND FOLLOW ON TESTING

13.1 Analytical Correction. While the many of previous sections of this manual discussed various techniques applicable to the design and development phases of the product lifecycle, it is also important to note that many of the same techniques can be utilized as the system matures. Even with the best foresight, testing and planning, operational failures still occur. However, utilization of HALT and PoF techniques can help to rapidly mitigate any concerns that should arise.

13.2 Intuition or Determination. Often times, when failure occurs, it is easy for the parties responsible for implementation of corrective actions to proceed from an intuitive approach in the failure investigation process. The traditional techniques involved in this process have been based on additional material testing, analysis based on hysteretic material fatigue findings, and engineering intuition.

When modeling efforts have occurred during the design and development phase, the mature and validated model may be leveraged to provide a more rapid investigation of the failure. Model inputs can be derived by either mimicking operating conditions during which the failure occurred, or by extrapolating increased load, environment or harshness inputs from existing data. Employing such techniques provides a direct, deterministic solution to the causation of the failure. Moreover utilization of inputs derived from dynamic modeling and test captured data sets can be utilized in FEA analysis of any part revisions conducted.

13.3 Reduction of Test-Fix-Test. Due to the relatively rapid nature of leveraging a validated model, corrective action identification through M&S efforts tends to reduce time between failure and implementation of corrective action. The modeling tools described here prior, when utilized to investigate and predict outcomes of corrective actions, tend to reduce test-fix-test iteration by giving the engineer and design team the complete picture of system-component interaction. Additionally, as the modeling effort is typically less time consuming and costly than development of revised “prototype” parts, modeling can analyze a number of proposed solutions and provide comparative results so that the best solution is available.

13.4 Support to Follow-On Testing. In the traditional product design life cycle, component and system failures have required additional follow-on testing in order to validate the effectiveness of any corrective actions. While validation is always warranted, planning and implementation of re-test can be lengthy and time consuming. To help expedite follow on testing, PoF and FEA analysis, coupled with HALT techniques can be utilized to expedite re-test, ensure critical data is recorded and often times lead to an overall reduction in re-test requirements due to the additional insight and knowledge provided by the modeling effort.

14. SUMMARY

The information contained here prior was developed to address the appropriate mathematical and engineering practices during the materiel acquisition process for new military systems. The reliability concepts and methodologies presented within this guide have evolved from accepted commercial practice and actual application to Army, Marine, Navy and Air Force systems during their associated design and re-design lifecycles. Written as an overview for both the manager and the analyst, the information contained within should serve as a more detailed explanation of the techniques and requirements of the DFR process. It is hoped that the guidance presented can be utilized to enhance current design reliability practices and provide a guideline for the development of best engineering practices.

This manual is intended to provide a general understanding of the concepts and principles required, and serve as an outline to robust design, however it is not meant to be employed without project specific tailoring. An end user should apply the appropriate methods in conjunction with their specific project goals and needs. The manual should serve as a basis for identification and planning of the appropriate process steps that can be utilized during the design process. Process step alignment to typical development timeline has been discussed within the text, and is also provided via the guidance from the GEIA-STD-0009 derived Six Column Matrix found in the appendix. Application of the techniques discussed has been shown to streamline the design process, enhance the level of knowledge gained from test and improve the overall reliability of fielded systems. As such, it is hoped that the reader will find the provided guidance a benefit to their work in product reliability now and in the future.

15. NOTES

15.1 Intended use. This handbook provides guidance to help in the application of the Design for Reliability process steps through the acquisition process.

15.2 Superseding information. None.

15.3 Subject term (Keyword listing).

15.4 Changes from previous issue: Previous Issue Unavailable.

APPENDIX A - SIX COLUMN MATRIX

THIS PAGE INTENTIONALLY LEFT BLANK.

SIX COLUMN MATRIX

From	Input	Activities	Output/Product	To	0009
System Engineering architecture (Product structure and functional Decomposition)	<i>Design Concept</i> Ideal/Intended Functions	Bottom-up architectural diagram (Components/LRUs) Functional Decomposition	Bottoms up component level detail Finalize Architecture Development (Work Breakdown Structure) Bill of Materials	Parameter Diagram	Objective 2 (Early Post MS B)
SE Architecture & Trade Studies	Product boundaries and levels of Detail	Determine boundaries/interfaces/cause and effect relationships and factors that affect system performance Partition System into functional components and subsystems	Functional Block Diagram Error States Noise Factors Control Factors Unintended Functions	Parameter Diagram	
SE Functional Decomposition & Trade Studies	Physical and functional relationships among components/systems	Tolerance Analysis (environmental and physics stresses) Functional Decompositions/tolerance specifications Reliability Allocation (Component and Subsystem reliability requirements)	<i>Reliability Block Diagram</i>	Failure Definition Parameter Diagram	
CONOPS	Customer usage profile to establish performance-based reliability requirements.	Understand the scope and magnitude of the end-use environments and levels and frequency of stress exposures (temperature, humidity, shock, vibration and power) to which the product will be exposed throughout its useful life. Identify the natural and induced environmental characteristics that the product may experience in its life cycle Quantify the high and low extreme and rate of change conditions for each of the environmental stresses Determine the conditions that have the most impact.	<i>Characterization of Operational/Environmental Loads the product can be expected to experience.</i>	Failure Definition Ideal Function	
Failure Definition	Failure mechanisms Error States Reliability Block diagram Characterization of Operational/Environmental Loads the product can be expected to experience.	List of all relevant performance characteristics and the levels at which the product operation is considered unacceptable Fatigue modeling, design for environments, life characteristics	<i>Stakeholder consensus of product failure Definitions</i> S-N Curve	Parameter Diagram DFMEA/FMECA FTA DVP&R (Reliability DOE)	
Parameter Diagram	Noise Factors BOM Error States Ideal/Intended Functions	Failure Definition based DFMEA (Qualitative) BOM based FMECA (Quantitative) <i>Physics of Failure Analysis (PoF) of Pre-production design and components</i> <i>Finite Element Analysis</i> <i>Failure Prevention and Review Board</i>	Failure Modes (Failure sites and mechanisms) Root Causes <i>Critical Components (Prioritized List of FMs)</i> Recommended/Corrective Actions strategies Conceptual Design Refinement	DVP&R (Reliability DOE) DFMEA/FMECA FTA	
DVP&R (Reliability DOE)	Noise Factors S-N Curve	<i>HALT (Assemblies, sub-assemblies and components)</i> <i>HALT (system level)</i> Accelerated Life Testing (prototype) Environmental Testing (prototype) Reliability growth testing (prototype) Failure Prevention and Review Board	<i>Design Refinement</i> <i>Inherent Reliability Estimate from modeling and simulation along with lower level testing</i>	DFMEA/FMECA Closed Loop FRACAS	Objective 2 (Pre MS C)
FTA (system level-top down)	Functions Failure Modes	Identify single failure points Evaluate software and man-machine interfaces Evaluate design change impacts Ishikawa (fish-bone) Diagram	Qualitative measurement of the consequences and criticality of potential failures	DFMEA	
DFMEA/FMECA (component level-bottom up)	FMs Root Causes/Noise Factors Ideal/Intended Functions Control Parameters/Spec	FMEA based DVP&R (Reliability DOE) Root Cause Failure Analysis (System Level) Failure Prevention and Review Board Prioritization of Failure Modes	Reliability Demonstration/Verification Tests Reliability Growth Assessment with confidence	Low Rate Production	
Closed Loop FRACAS	Failures and corrective action information for hardware and software failure modes and mechanisms	Capture data to analytically assess in-process and end-use reliability Identify root failure causes Track the identification and implementation of corrective actions to eliminate the effect of failures on the inherent design reliability of the product. Failure Prevention and Review Board Prioritization of Failure Modes	Failure reports Failure analysis Failure modes Failure mode mitigation Risk mitigation decisions Configuration control Lessons learned	Low Rate Production	
FRCAS Low Rate Production	Reliability Estimation Control Parameters/Spec	HALT/ HASS of Production Articles POF Test Failures Failure Prevention and Review Board	Design Refinement Operational Reliability Estimate	FRCAS Follow on Test and Evaluation FRP and Fielding	

THIS PAGE INTENTIONALLY LEFT BLANK.