ORGANIZATIONAL MISSION ASSURANCE STANDARD

Mission Assurance Program

Revision: 1 Release: 01-02-2011 Effective: 01-02-2011

SET

STANDARD

OBJECTIVE

This Standard defines SET's approach for implementing a Mission Assurance Program (MAP). Through the interpretation and implementation of this Standard SET shall tailor its System Safety Program, Reliability, Maintainability, Availability and Dependability (RMAD) Program, and Quality Assurance Program to achieve all pertinent mission assurance requirements which are commensurate with the unit-value category of its products. At the time this Standard was written SET did not develop any very-high or ultra-high unit-value products.

Note: Guidance for product unit-value determination is found in Figure 1.

APPLICABILITY

This Standard applies to all present and future SET sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a MAP has been contractually imposed.

Note: The terms and acronyms used in this Standard are defined in Section 3.

1. Introduction

This Standard establishes the general requirements for a Mission Assurance Program (MAP).

1.1 Scope

This Standard applies to all present and future SET™ sites/facilities, programs/projects, business lines/services, functional organizations/working groups, and employees/subcontractors, regardless of whether a MAP has been contractually imposed.

1.2 Purpose

Mission assurance is the project-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to mission success, throughout the product life cycle. A MAP is a set of interrelated processes that have the capability of assessing and eliminating or controlling predefined deficiencies for a specific product. These deficiencies include damage-threatening hazards, mission-impacting failures modes, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors. Through the interpretation and implementation of this Standard, SET shall implement mission assurance programs which are tailored to achieve all pertinent mission assurance requirements which are commensurate with the unit-value category of its products.

The provisional AIAA Standard S-102.0.1 (Draft), *Mission Assurance Program General Requirements*, partitions mission assurance into three principal components, safety, reliability and quality assurance (SR&QA). SET rephrases the definitions of these mission assurance components to be more precise yet more generally applicable in context of the SET product line.

1. Safety is the measure of the interaction of a product function with all other infrastructures, with or without a defined interface, to avoid accidents. Accidents are an unintentional intersection of dissimilar infrastructures, or like structures at somewhere other than the proper interface.

2. Reliability is the measure of the functional integrity of a product on a sustained basis. Sufficient reliability certainly for supporting the mission during the specified duration.
3. Quality assurance is the measure of control over processes applied to the product, over attributes of the product, and over services which the product's functions provide.

1.3 Applicability

SET's strengths in systems analysis, architecture and design are consistent and coherent. Yet the application of mission assurance practices in past technology development was hit-and-miss. Based upon sage advice and cogent reasoning since then, the SET™ has embarked on a company-wide endeavor to integrate and apply mission assurance in general, and SR&QA in particular, throughout the company's systems engineering processes. These processes are judiciously applied in the development of all its products. The criteria for rating products in accordance with a defined scale of product unit-values are found in the provisional AIAA Standard S-102.1.1, *Mission Assurance Program Planning Requirements*. The product unit-value criticality categorization that applies to this Standard is shown in Figure 1.

Figure 1. AIAA Defined Product Unit-Value Criticality Categorization.

Ultra-High Unit-Value	Very-High Unit-Value	High Unit-Value	Medium Unit-Value	Low Unit-Value
• Defense satellites • Launch vehicles • Long-range missiles • Nuclear weapons • Nuclear power plants • Manned spacecraft	• Commercial / communications satellites • Fossil fuel / hydro-electric power plants • Oil tankers • Off shore oil rigs • Water filtration plants • Short-range missiles/rockets • Passenger aircraft / helicopters • Military aircraft / helicopters • Military drones / unmanned vehicles • Naval vessels • Passenger trains / buses • Cruise liners • Safety-critical hardware / software components • Satellite ground control stations	• Science satellites • Cargo ships • Mobil / mechanized weapons • Freight trains • Amusement park rides • Elevators / escalators • Small private aircraft / helicopters • Automobiles / trucks / motorcycles • Mission-critical hardware / software components • Construction / demolition / excavation equipment • Satellite communications relay stations	• Industrial electronics • Personal computers / peripherals • Industrial computers / peripherals • Farm equip • Medical / laboratory equip • Factory machinery • Handheld construction / demolition / excavation equip • Communications / utility equip • Explosive devices • Test / monitoring hardware/software components • Computer operating system software • Prototype systems / components	• Motorized / manual hand tools • Fire arms • Consumer electronics • Household appliances • Batteries • Battery operated toys • Infant/ children toys • Computer application program software

2. REFERENCES

2.1 Normative References

The following reference documents of the issue in effect on the date on invitation for bid or request for proposal form a part of this Standard to the extent specified:

AIAA S-102.1 Mission Assurance Management

1) AIAA S-102.0.1 (Draft)	Mission Assurance Program (MAP) General Requirements
2) AIAA S-102.1.1 (Draft)	Mission Assurance Program Planning (MAPP) Requirements
3) AIAA S-102.1.2 (Draft)	Subcontractor and Supplier Mission Assurance Management Requirements
4) AIAA S-102.1.3 (Draft)	Mission Assurance Working Group (MAWG) Requirements
5) AIAA S-102.1.4 (Released)	Failure Reporting, Analysis and Corrective Action System (FRACAS) Requirements
6) AIAA S-102.1.5 (Released)	Failure Review Board (FRB) Requirements
7) AIAA S-102.1.6 (Draft)	Critical Item Risk Management (CIRM) Requirements
8) AIAA S-102.1.7 (Draft)	Project Mission Assurance Database System Requirements
9) AIAA S-102.1.8 (Draft)	Quality Assurance (QA) Requirements
10) AIAA S-102.1.9 (Draft)	Configuration Management (CM) Requirements
11) AIAA S-102.1.10 (Draft)	Environmental Safety Assurance Requirements

AIAA S-102.2 Mission Assurance Engineering and Analysis

12) AIAA S-102.2.1 (Draft)	Functional Diagram Modeling (FDM) Requirements
13) AIAA S-102.2.2 (Released)	System Reliability Modeling Requirements
14) AIAA S-102.2.3 (Draft)	Component Reliability Predictions Requirements
15) AIAA S-102.2.4 (Released)	Product Failure Mode, Effects and Criticality Analysis (FMECA) Requirements
16) AIAA S-102.2.5 (Draft)	Sneak Circuit Analysis (SCA) Requirements
17) AIAA S-102.2.6 (Draft)	Design Concern Analysis (DCA) Requirements
18) AIAA S-102.2.7 (Draft)	Finite Element Analysis (FEA) Requirements
19) AIAA S-102.2.8 (Draft)	Worst Case Analysis (WCA) Requirements
20) AIAA S-102.2.9 (Draft)	Human Error Predictions Requirements
21) AIAA S-102.2.10 (Draft)	Environmental Event Survivability Analysis Requirements

22) AIAA S-102.2.11 (Released) Anomaly Detection and Response Analysis Requirements

23) AIAA S-102.2.12 (Draft) Maintainability Predictions Requirements

24) AIAA S-102.2.13 (Draft) Operational Dependability and Availability Modeling Requirements

25) AIAA S-102.2.14 (Draft) Hazard Analysis (HA) Requirements

26) AIAA S-102.2.15 (Draft) Software Component Reliability Predictions Requirements

27) AIAA S-102.2.16 (Draft) Process Failure Mode, Effects, and Criticality Analysis (FMECA) Requirements

28) AIAA S-102.2.17 (Draft) Event Tree Analysis (ETA) Requirements

29) AIAA S-102.2.18 (Draft) Fault Tree Analysis (FTA) Requirements

30) AIAA S-102.2.19 (Draft) Fishbone Analysis Requirements

31) AIAA S-102.2.20 (Draft) Similarity and Allocations Analysis Requirements

32) AIAA S-102-2.21 (Draft) Component Engineering Requirements

33) AIAA S-102.2.22 (Draft) Stress and Damage Simulation Analysis Requirements

AIAA S-102.3 Mission Assurance Testing

34) AIAA S-102.3.1 (Draft) Environmental Stress Screening (ESS) Requirements

35) AIAA S-102.3.2 (Draft) Reliability Development / Growth Testing (RD/GT) Requirements

36) AIAA S-102.3.3 (Draft) Reliability, Maintainability, and Availability Demonstration Testing Requirements

37) AIAA S-102.3.4 (Draft) Reliability Life Testing Requirements

38) AIAA S-102.3.5 (Draft) Design of Experiments Requirements

39) AIAA S-102.3.6 (Draft) Ongoing Reliability Testing (ORT) Requirements

40) AIAA S-102.3.7 (Draft) Product Safety Testing Requirements

Corporate References

41) Reliability Design Rules (Draft)

2.2 Relationship to Other Corporate Standards

This Standard overarches the Corporate Standards for the System Safety Program, the Reliability, Maintainability, Availability & Dependability (RMAD) Program, and the Quality Assurance (QA) Program. This Standard defines the purposes of the processes which are included in the lower tier programs. Each of the lower tier program standards defines the set of activities that aid identification, evaluation, and mitigation or control of existing and potential deficiencies of low, medium, and high unit-value products.

3. Terminology

3.1 Terms and Definitions

anomaly
apparent problem or failure affecting a configured product, process, or support equipment/facilities that is detected during product verification or operation
NOTE: Anomalies are distinguished from discrepancies, product defects which do not violate project requirements which may or may not be documented in the FRACAS.

acquisition authority
an organization (Government, contractor, or subcontractor) that levies requirements on another organization through a contract or other document

approximation[1]
a value that is nearly but not exactly correct or accurate

audit
an independent examination of accounts and records to assess or verify compliance with specifications, standards, contractual agreements, or other criteria (Ref. IEEE STD 1624-2008)

baseline process
the minimum set of functions that constitute a specific type of process

baseline program
the minimum set of functions that constitute a specific type of program

capability
one or more processes or activities that describe how SR&QA programs are used, treated, or developed within an organization (Ref. IEEE STD 1624-2008)

capability-based mission assurance program
the set of processes that assesses and controls product deficiency risk at one or more predefined capability levels

capability level
measure of the ability of a mission assurance process, as specified by a set of activities, to address the pertinent mission assurance needs of a systems engineering process

[1] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

capability level growth
a measurable improvement (e.g., an increase in resources, scope of effort, or maturity of input data) in the ability of a mission assurance process to support the mission assurance needs of a systems engineering process

chaos
the random occurrence of unpredictable and unrelated events

control
a method used to reduce the consequences, likelihood, or effects of a hazard or failure mode
NOTE: Controls include special design features, procedures, inspections, or tests

credible failure mode or hazard
a failure mode or hazard with a probability of occurrence greater than 1.0E-6, 0.000001, or one in a million

engineering judgment
a properly trained engineer's technical opinion that is based on an evaluation of specific data and personal experience
NOTE: Engineering judgments are a reality that cannot not be avoided when insufficient time, data, or funding are available to perform a detailed quantitative analysis. (See Sections 5.5.1 and 5.5.2 for more information.)

environmental safety assurance
to give appropriate consideration to potential environmental impacts prior to beginning any action that may significantly affect the environment

estimation
a tentative evaluation or rough order magnitude calculation

failure
termination of the ability of a unit to perform its required function
NOTE: A fault may cause a failure.

failure mode
consequence of the mechanism through which a failure occurs, or the manner by which a failure is observed

fault[2]
[1] [Software reliability] a manifestation of an error in software; [2] [Hardware reliability] any undesired state of a component or system; [3] [Components] a defect or flaw in a hardware or

[2] Definition source: IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*

software component; [4] [Human reliability] procedure (operational or maintenance) or process (manufacture or design) that is improperly followed;
NOTES: [1] An accident may cause a fault; [2] A fault may cause a failure; [3] A fault does not necessarily require failure.

hazard
a condition that is prerequisite to a mishap and a contributor to the effects of the mishap
NOTE: A single point failure mode (SPFM) item is a hazard with respect to its potential to lead directly to loss of a safety-critical or mission-critical system function.

maturity level
measure of the degree of accuracy of a data product, as developed using a specified set of input data, in relation to what is considered the best achievable results

method
a formal, well-documented approach for accomplishing a task, activity, or process step governed by decision rules to provide a description of the form or representation of the outputs (C/SE) 1220-1994s

mishap
an unplanned event or series of events resulting in death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

mission
the purpose and functions of the space system (sensors, transponders, boosters, experiments, etc.) throughout its expected operational lifetime, and controlled reentry or disposal orbit time period. A space system may have multiple missions (e.g., primary mission, ancillary mission, and safety mission)

mission assurance
the program-wide identification, evaluation, and mitigation or control of all existing and potential deficiencies that pose a threat to system safety or mission success, throughout the product's useful life and post-mission disposal
NOTE: Deficiencies include damaging-threatening hazards, mission-impacting failures, and system performance anomalies that result from unverified requirements, optimistic assumptions, unplanned activities, ambiguous procedures, undesired environmental conditions, latent physical faults, inappropriate corrective actions, and operator errors.

mission capability
This term encompasses the purpose and functions of the space system (sensors, transponders, etc.) throughout its intended system mean mission duration (the expected life of the space vehicle). (Ref. AFMAN 91-222 SUPL1)

mitigation
(1) a method that eliminates or reduces the consequences, likelihood, or effects of a hazard or failure mode; (2) a hazard control

modeling
act of producing a representation or simulation of one or more items

non-credible failure mode or hazard
a failure mode or hazard with a probability of occurrence equal to or less than 1.0E-6, 0.000001, or one in a million
NOTE: In System Safety Engineering, the qualitative probability values of an improbable hazard and a non-credible hazard are equivalent.

plan
a method for achieving an end

practice
one or more activities that use specified inputs to develop specified work products for achieving specified objectives (Ref. IEEE Standard 1624-2008)

process-based lesson learned
important information created, documented, and retrieved according to a process or procedure descriptor

product-based lesson learned
important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor
program
[1] the managed collection of an organization’s practices that is structured to ensure that the customers’ requirements and product needs are satisfied (Ref. IEEE Standard 1624-2008); [2] a defined set of managed processes conducing to an end under a single plan
NOTE: A program does not have to consist of related, managed process. Compare with definition of *“system”*.

process
a sequence of tasks, actions, or activities, including the transition criteria for progressing from one to the next, that bring about a result (Ref. IEEE Standard 1624-2008)

NOTE: A process can be unmanaged or managed. An unmanaged or "free" process does not have its inputs or outputs controlled. The rain and melted snow that replenishes a lake is an example of an unmanaged process. A managed or "controlled" process has its inputs and outputs controlled. An electrical power station is an example of a managed process.

quality
a measure of a part's ability to meet the workmanship criteria of the manufacturer
NOTE: Quality levels for parts used by some of the handbook methods are different from quality of the parts. Quality levels are assigned based on the part source and level of screening the part goes through. The concept of quality level comes from the belief that screening improves part quality.

reliability
probability that an item will perform its intended function for a specified interval under stated conditions

residual risk
risk associated with significant failure modes or hazards for which there are no known control measures, incomplete control measures, or no plans to control the failure mode or hazard

root cause(s)
most fundamental reason(s) an event might or has occurred

root cause analysis
a process for identifying the fundamental cause of an event or failure

safety
freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment

safety critical
a term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component

specialty engineering
a subgroup of the engineering processes that make up the Mission Assurance Process
Note: Traditionally, this subgroup includes Reliability, Maintainability, PMP, Survivability, and Supportability.

system
[1] a defined set of related processes
[2] elements of a composite entity, at any level of complexity of personnel, procedures, materials, tools, equipment, facilities, and software, that are used together in an intended

operational or support environment to perform a given task or achieve a specific purpose, support, or mission requirement
NOTE: A system that consists of one or more unmanaged processes is susceptible to becoming "unbalanced" and changing over time (e.g., an ecological system). For a system to maintain stability it must be "balanced" and consist only of managed processes.

system safety
the application of engineering management principles, criteria, and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system lifecycle (Ref. MIL-STD-882C)

systems engineering
An interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and life-cycle balance set of system product and process solutions that satisfy customer needs. (Ref. MIL-STD-499B Draft)

tailoring
process by which the individual requirements (tasks, sections, paragraphs, words, phrases, or sentences) of a standard are evaluated to determine the extent to which each requirement is most suited for a specific system acquisition and the modification of these requirements, where necessary, to ensure that each tailored document invokes only the minimum needs of the customer

timely
performance of a task, subtask, or effort when planning and execution results in the output being provided with sufficient time for management, if need be, to identify and implement cost-effective action
EXAMPLE: An action that avoids or minimizes schedule delays and cost increases.

validation
the act of determining that a product or process, as constituted, will fulfill its desired purpose
verification
the process of assuring that a product or process, as constituted, complies with the requirements specified for it

3.2 Acronyms

A_O	Availability Analysis
CA	Criticality Analysis
CIRM	Critical Item Risk Management
CN	Criticality Number
DCA	Design Concern Analysis

D_O	Dependability Analysis
ESS	Environmental Stress Screening
ETA	Event Tree Analysis
ETC	Estimate to Complete
FDM	Functional Diagram Modeling
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode, Effects, and Criticality Analysis
FRACAS	Failure Reporting, Analysis, and corrective Action
FRB	Failure Review Board
FTA	Fault Tree Analysis
HA	Hazard Analysis
HW	Hardware
LLAA	Lessons Learned Approval Authority
LOE	Level of Effort
MAP	Mission Assurance Program
	Mission Assurance Process
MAPP	Mission Assurance Program Plan
	Mission Assurance Program Planning
MAWG	Mission Assurance Working Group
MCLP	Multiple Capability Level Process
PMP	Parts, Materials & Processes
PoF	Physics of Failure
QA	Quality Assurance
R&M	Reliability and Maintainability
RD/GT	Reliability Development/Growth Testing
RMAD	Reliability, Maintainability, and Availability Demonstration
	Reliability, Maintainability, Availability and Dependability
SCA	Sneak Circuit Analysis
SCLP	Single Capability Level Process

SEC	Standards Executive Council
SPFM	Single Point Failure Mode
SR&QA	Safety, Reliability & Quality Assurance
SSP	System Safety Program
SW	Software
TAAF	Test, Analyze and Fix
V&V	Verification & Validation

4. General Requirements

Typically, mission assurance is ventured into by a company without a definite plan of implementation. At best, the typical company implements a fragmented, unstructured reliability program that leads to lower than desired operation reliability of fielded systems. To avoid this undesired situation, SET has adopted the AIAA S-102 Mission Assurance Standards. These standards provide the foundation for tailoring the Mission Assurance Program (MAP) to be commensurate with the unit-value and life cycle phase of the product that it is applied to. Accordingly, SET's MAPs shall be implemented in accordance with the groups of "capability-based" processes shown in Figures 2, 3 and 4. Figure 2 shows SR&QA MAPs for low unit-value products, Figure 3 shows SR&QA MAPs for medium unit-value products, and Figure 4 shows SR&QA MAPs for high unit-value products. This "capability-based" approach to mission assurance is cost-effective and repeatable, and as such, will be extensible into pristine technical territory in the future.

The MAPs implemented by SET during product development focus on optimizing inherent reliability requirements, and verifying those requirements are met at a specified time prior to delivery. A long range goal of SET is to provide mission assurance services which focus on optimizing operational reliability requirements, and verifying those requirements are met at a specified time after product delivery. The mission assurance models built during product development would become customer service tools after the product is delivered. The post-delivery mission assurance services would aid customers to improve the operational reliability of fielded systems through an iterative process of test, analyze and fix (TAAF). When the TAAF process is applied in a structured manner to improve operational reliability it is known as Reliability Development / Growth Testing (RD/GT).

The input data for RD/GT primarily comes from two types of sources: 1) databases which contain mission assurance data generated during development of the delivered product, and 2) databases which contain performance and failure data collected during operation of the fielded product. SET offers its customers access to a **mission assurance portal** that can link with their internal databases, for the purpose of 1) downloading performance and failure data to assess operational reliability metrics, and 2) uploading root cause and corrective action data to implement reliability growth features. The **mission assurance portal** can be easily modified to accommodate the data formats of customers and clients, which would facilitate efforts to cross-validate results.

The **mission assurance portal** shall be the aggregation of a project's mission assurance database system. It is essentially a set of SET resources that is used to assess reliability growth. The product's major stake-holders shall collaborate in specifying the detailed requirements and architecture of each **mission assurance portal**. At a minimum, the **mission assurance portal** shall be capable of downloading all performance and failure data which pass through external interfaces, both inputs and outputs, of the fielded product, and is pertinent to reliability growth of that product. The Mission Assurance Implementation Matrix of Table 1 shows the kinds of SR&QA products, sorted by domain, in each of the management levels within SET. Figure 2 shows SET's product support portal process flow.

Table 1. Mission Assurance Implementation Matrix

Domains	System Safety	Reliability, Maintainability, Availability & Dependability	Quality Assurance
Corporate / Organizational	Company-internal system safety standards / tools, training, and associated databases	Company-internal RMAD standards / tools, training, and associated databases	Company-internal product qualification and customer support standards / tools, training, and associated databases
Programs / Projects	Developmental product's system safety program planning, safety design / operations analyses, verifications, and associated databases	Developmental product's RMAD program planning, reliability design / operations analyses, verifications, and associated databases	Developmental product's qualification, customer support planning, and associated databases
Product Mission Assurance Portal	Operational product's safety-critical software, system safety tools / heritage data, documented procedures, assessments, consulting, and training	Operational product's mission-critical software, RMAD tools / heritage data, documented procedures, assessments, consulting, and training	Operational product's customer support, customer / subcontractor auditing, and associated databases

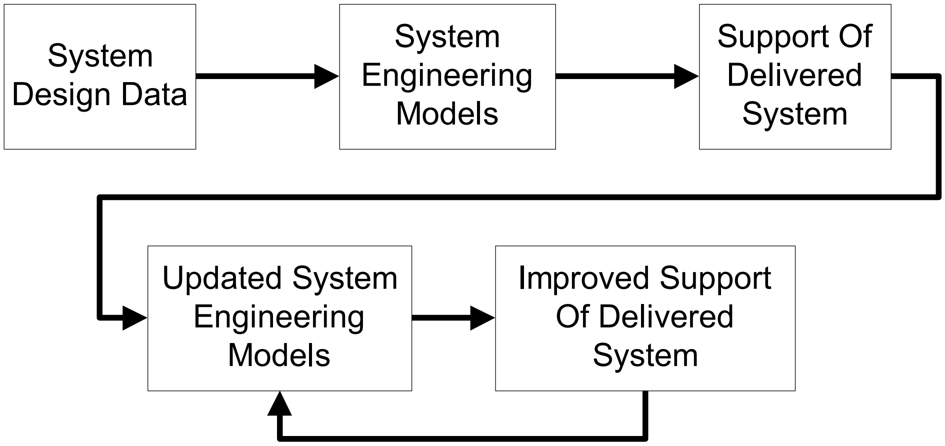
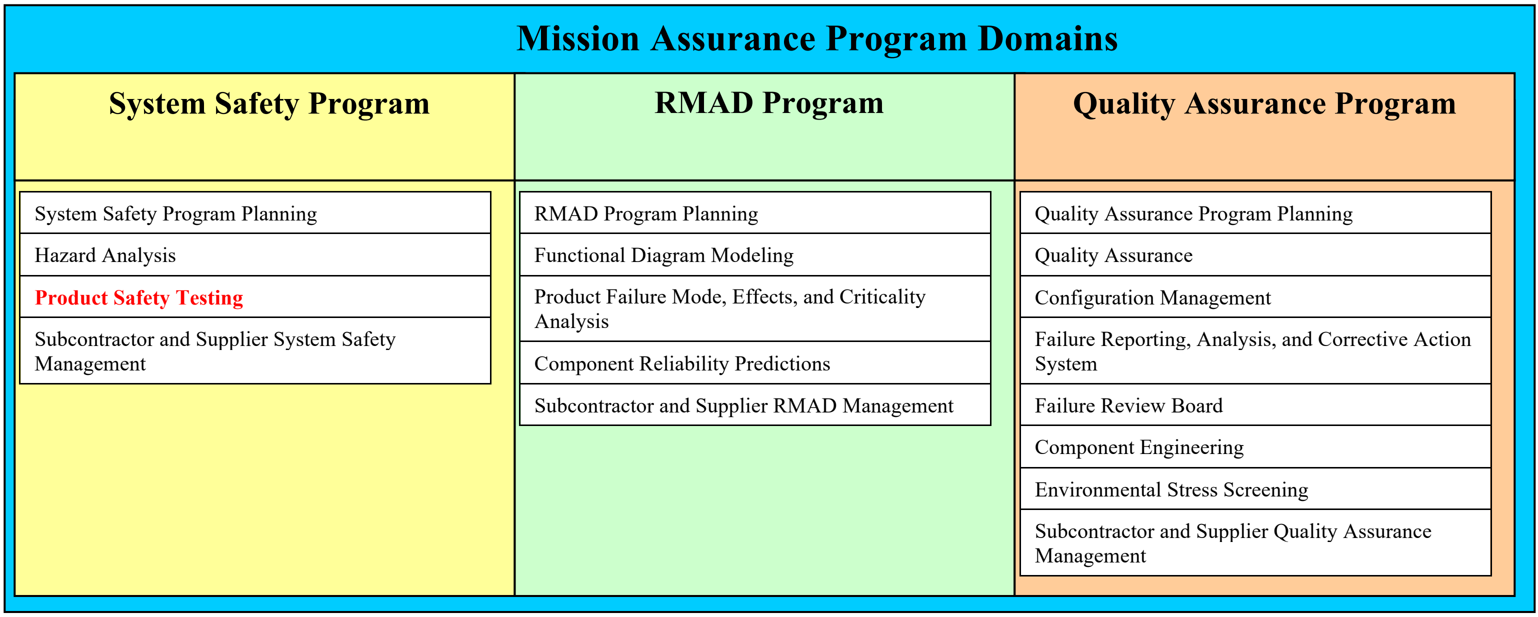

System Design Data
System Engineering Models
Support Of Delivered System
Updated System Engineering Models
Improved Support Of Delivered System

Figure 2. SET's Product Support Portal Process Flow.

The success of a company's mission assurance efforts is entirely dependent upon its commitment of the corporate culture to mission assurance at all levels and scales of the company's existence. The degree of effectiveness of this institutionalized mission assurance mindset is most frequently referred to as **organizational mission assurance capability**. Synonymous with **organizational mission assurance capability** is **organizational reliability capability**, which is defined by IEEE Standard 1624-2008 as the ability of an organization's reliability practices to ensure that product reliability meets or exceeds its customers' requirements.

A mission assurance mantra, slideshow or banner would not aid the delivery of a reliable product, unless they somehow guide product developers in the application of cost-effective and repeatable methodologies which assure safe and reliable software, hardware and operations products. A more plausible source for such guidance would be industry or military standards. The exemplary MAP is one that is based on standards which are capable of achieving an optimal balance between product safety, product reliability, and product cost, whether accrued during design, manufacture, integration, delivery, or customer use.

Figure 3. Low Unit-Value Product Mission Assurance Program Domains (Notional)



Mission Assurance Program Domains

System Safety Program	RMAD Program	Quality Assurance Program
System Safety Program Planning	RMAD Program Planning	Quality Assurance Program Planning
Hazard Analysis	Functional Diagram Modeling	Quality Assurance
Product Safety Testing	Product Failure Mode, Effects, and Criticality Analysis	Configuration Management
Subcontractor and Supplier System Safety Management	Component Reliability Predictions	Failure Reporting, Analysis, and Corrective Action System
	Subcontractor and Supplier RMAD Management	Failure Review Board
		Component Engineering
		Environmental Stress Screening
		Subcontractor and Supplier Quality Assurance Management

Figure 4. Medium Unit-Value Product Mission Assurance Program Domains (Notional)

Mission Assurance Program Domains

System Safety Program	RMAD Program	Quality Assurance Program
System Safety Program Planning	RMAD Program Planning	Quality Assurance Program Planning
Hazard Analysis	Functional Diagram Modeling	Quality Assurance
Product Safety Testing	Product Failure Mode, Effects, and Criticality Analysis	Configuration Management
Subcontractor and Supplier System Safety Management	Component Reliability Predictions	Failure Reporting, Analysis, and Corrective Action System
	Software Component Reliability Predictions	Failure Review Board
	Design Concern Analysis	Project Mission Assurance Database System
	Worst Case Analysis	Component Engineering
	Environmental Event / Survivability Analysis	Environmental Stress Screening
	System Reliability Modeling	Subcontractor and Supplier Quality Assurance Management
	Maintainability Predictions	
	Subcontractor and Supplier RMAD Management	

Figure 5. High Unit-Value Product Mission Assurance Program Domains (Notional)

Mission Assurance Program Domains

System Safety Program	RMAD Program	Quality Assurance Program
System Safety Program Planning	RMAD Program Planning	Quality Assurance Program Planning
Hazard Analysis	Functional Diagram Modeling	Quality Assurance
Event Tree Analysis	Product Failure Mode, Effects, and Criticality Analysis	Configuration Management
Fault Tree Analysis	Component Reliability Predictions	Failure Reporting, Analysis, and Corrective Action System
Product Safety Testing	Software Component Reliability Predictions	Failure Review Board
Subcontractor and Supplier System Safety Management	Design Concern Analysis	Project Mission Assurance Database System
System Safety Working Group	Worst Case Analysis	Component Engineering
	Environmental Event / Survivability Analysis	Critical Item Risk Management
	System Reliability Modeling	Environmental Stress Screening
	Maintainability Predictions	Subcontractor and Supplier Quality Assurance Management
	Anomaly, Detection, and Response Analysis	Quality Assurance Working Group
	Operational Dependability and Availability Modeling	
	Similarity and Allocations Analysis	
	Reliability Life Testing	
	Subcontractor and Supplier RMAD Management	
	RMAD Working Group	

Figure 6. Very-High Unit-Value Product Mission Assurance Program Domains (Notional)

Mission Assurance Program Domains		
System Safety Program	**RMAD Program**	**Quality Assurance Program**
System Safety Program Planning	RMAD Program Planning	Quality Assurance Program Planning
Hazard Analysis	Functional Diagram Modeling	Quality Assurance
Event Tree Analysis	Product Failure Mode, Effects, and Criticality Analysis	Configuration Management
Fault Tree Analysis	Component Reliability Predictions	Failure Reporting, Analysis, and Corrective Action System
Product Safety Testing	Software Component Reliability Predictions	Failure Review Board
Environmental Safety Assurance	Design Concern Analysis	Project Mission Assurance Database System
Subcontractor and Supplier System Safety Management	Worst Case Analysis	Component Engineering
System Safety Working Group	Environmental Event / Survivability Analysis	Critical Item Risk Management
	System Reliability Modeling	Environmental Stress Screening
	Maintainability Predictions	Fishbone Analysis
	Anomaly Detection and Response Analysis	Subcontractor and Supplier Quality Assurance Management
	Operational Dependability and Availability Modeling	Quality Assurance Working Group
	Similarity and Allocations Analysis	
	Stress and Damage Simulation Analysis	
	Finite Element Analysis	
	Sneak Circuit Analysis	
	Reliability Life Testing	
	Reliability Development / Growth Testing	
	Reliability, Maintainability, and Availability Demonstration Testing	
	Process Failure Mode, Effects, and Criticality Analysis	
	Subcontractor and Supplier RMAD Management	
	RMAD Working Group	

5. DETAILED REQUIREMENTS

The following detailed requirements pertain to Mission Assurance Programs of equivalent capability, as defined by Annex B.

5.1 Authorize Mission Assurance Program

For all products regardless of unit-value criticality, SET shall assign the authority and responsibility for meeting the mission assurance requirements and objectives to a minimum of three independent programs:

- System Safety Program
- Reliability, Maintainability, Availability, and Dependability (RMAD) Program
- Quality Assurance (QA) Program

If a System Safety Program, RMAD Program, or QA Program is not authorized in a project, or only partially authorized with regard to this Standard, then it shall be the responsibility of the lead Safety/Reliability/Quality Engineer to provide documented evidence that verifies only negligible or non-credible faults / weaknesses exist in the system/processes.

5.1.1 System Safety Program

The System Safety Program shall be authorized in accordance with this Standard, and managed independent of the project's management chain, with responsibility and authority to 1) ensure all environmental, safety, and occupational health (ESOH) requirements are met, 2) evaluate potential ESOH hazards across the product life cycle, as applicable, and 3) implement identified operating, manufacturing, and maintenance safety procedures. The implementation of a System Safety Program, to evaluate potential hazards during the design, manufacture, assembly, testing, transportation, and operational phases of all high unit-value products, shall be required by contract or by organizational standards. If a System Safety Program is not implemented or only partially implemented in an acquisition project, then the responsible System Safety Engineer (SSE) must provide documented evidence that verifies only negligible or non-credible hazards exist in the product areas not evaluated.

5.1.2 Reliability, Maintainability, Availability, and Dependability Program

The RMAD Program shall be authorized in accordance with this Standard, with responsibility and authority to 1) ensure all reliability, maintainability, availability, and dependability risks are balanced within the project's objectives, constraints, and budget, 2) evaluate potential failure modes across the product life cycle, as applicable, and 3) quantify the inherent and operational reliability of the product. The implementation of an RMAD Program to evaluate potential failure modes during the design, manufacture, assembly, testing, transportation, and operational phases of all high unit-value products, shall be required by contract or by organizational standards. If an RMAD Program is not implemented or only partially implemented in an acquisition project, then the responsible Reliability Engineer (RE) must provide documented evidence that verifies only negligible or non-credible failure modes exist in the product areas not evaluated.

5.1.3 Quality Assurance Program

The QA Program shall be authorized in accordance with this Standard, and managed independent of the project's management chain, with responsibility and authority to 1) ensure all quality assurance requirements are met, and 2) evaluate potential processing faults / weaknesses across the product life cycle, as applicable. The implementation of a QA Program to evaluate potential processing faults / weaknesses during the design, manufacturing, testing, transportation, integration, and operational phases of all high unit-value products, shall be required by contract or by organizational standards. If a QA Program is not implemented or only partially implemented in an acquisition project, then the responsible Quality Engineer (QE) must provide documented evidence that verifies only negligible or non-credible faults / weaknesses exist in the processing areas not evaluated.

5.1.4 Assign Qualified Mission Assurance Management and Engineering Personnel

SET shall assign a qualified individual to manage the mission assurance program. The MAP manager shall ensure that appropriate engineering support is available to properly assess product and process life cycle deficiencies. SET shall provide validated tools, which are selected by the MAP manager, to aid the program-wide identification and elimination or control of unacceptable deficiencies. The tools shall provide the System Safety, RMAD, and QA programs, as well as other programs in the systems engineering process, with a standardized methodology for analyzing program issues, addressing technical questions, identifying improvements, and resolving problems. The tools shall also allow mission assurance programs to improve the comprehensiveness, accuracy, timeliness, repeatability, and cost-effectiveness of analyses. These tools shall facilitate the following objectives:

1. Automate the exchange of mission assurance data to the greatest extent practical.
2. Minimize both the size of SET's permanent mission assurance staff and the cost of acquiring and maintaining the mission assurance tools they use.

If a Capability Level 4 or above MAP is required, SET shall establish the minimum qualifications required to perform each mission assurance process.

5.1.5 Continuously Improve the Mission Assurance Process

If a Capability Level 5 or above MAP is required, SET shall establish an approach for continuously improving the mission assurance processes. At a minimum this approach shall include the following activities:

- Instituting procedures to facilitate the proactive identification and implementation of needed improvements in MA processes;
- Periodically training management and engineering personnel in the use of MA tools and the cost-effective implementation of MA processes.
- Integration of mission assurance lessons learned into the training materials.

5.2 Define/Identify and Flow Down the Mission Assurance Requirements

SET shall define/identify the mission assurance requirements that are consistent with the system requirements and this Standard, and flow them down to all affiliated subcontractors. If a Capability Level 2 or above MAP is required, SET shall document these requirements in approved mission assurance program plans.

If a System Safety Program, RMAD Program, or QA Program is not implemented or only partially implemented in a high-unit value acquisition project, then the responsible Safety/Reliability/Quality Engineer must provide documented evidence that verifies only negligible or non-credible faults/ weaknesses exist in the processing areas not evaluated.

The disposition of conflicting mission assurance requirements shall be based on the following requirements order of precedence:

1. Safety critical
2. Mission critical
3. Reliability critical
4. Maintenance critical
5. Monitoring critical

5.2.1 Identify the Mission Assurance Requirements Which Are Already Met

SET shall identify any mission assurance requirements which may be satisfied already by an existing analysis, inspection, test report, or data product from a similar project, product, or process. If a Capability Level 2 or above MAP is required, SET shall document these requirements in approved mission assurance program plans. If SET chooses to use results from a mission assurance process in another project for verification, then an explanation of how those results apply shall be provided by SET.

5.3 Planning the Mission Assurance Program

SET shall plan the mission assurance program to be commensurate with the unit-value criticality and life cycle phase of the product that it is applied to. Accordingly, SET's MAP shall be implemented in accordance with the groups of capability-based MAP domains shown in Figures 3 thru 7. These figures show the minimum processes that are required to be implement in the systems engineering life cycle of a product with a particular unit-value criticality. AIAA Standard S-102.1.1, *Mission Assurance Program Planning Requirements*, provides a breakdown of the processes that are required to be implemented in a particular systems engineering life cycle phase.

5.3.1 Select Mission Assurance Processes Based on Product Unit-Value Criticality

SET shall select the mission assurance processes that are commensurate with the product unit-value criticality, the systems engineering life cycle phase, the mission assurance requirements, and the capability level definitions in Appendix B. Collectively, the selected processes shall be capable of identifying all unacceptable product deficiencies, as defined mutually by SET and the customer in the Mission Assurance Program Plan. The following product characteristics shall be considered to be unacceptable deficiencies for unit-value criticality level 3 and above systems. Positive action and implementation verification is required to reduce the risk to an acceptable level as negotiated by SET and the customer.

a. Single component failure, common mode failure, human error, or design features which could cause a mishap of catastrophic or critical severity.

b. Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of catastrophic or critical severity.

c. Generation of hazardous ionizing/non-ionizing radiation or energy when no provisions have been made to protect personnel or sensitive subsystems from damage or adverse effects.

d. Packaging or handling procedures and characteristics which could cause a mishap for which no controls have been provided to protect personnel or sensitive equipment.

e. Hazard level categories that are specified as unacceptable in the contract.

f. Human factors capabilities. Component designs or locations that fail to address human physical, anthropometrics, physiological and perceptual-cognitive capabilities or limitations. For example, a design that is conducive to error, such as, controls that are difficult to read, are confusing, or create excessive cognitive demands on the users.

5.3.2 Select Mission Assurance Process Activities Based on Relevant Systems Engineering Life Cycle Phases

After identifying the general mission assurance processes based on the end product's unit-value criticality, SET shall identify the detailed mission assurance activities based on the interactions among the mission assurance processes and other functions in the systems engineering process. Specifically, SET shall identify (1) the mission assurance activities that are to be performed in each product life cycle phase; (2) the key inputs of each mission assurance activity, and the source of each key input; (3) the key outputs of each mission assurance activity, and the uses of each key output; (4) the estimated-time-to-complete (ETC) or level-of-effort (LOE) in hours for each mission assurance activity; (5) the key mission assurance milestones in each product life cycle phase; and (6) the program-wide risk management approach, i.e., the methods for monitoring, evaluating, reporting, and responding to anticipated and unanticipated problems.

The mission assurance programs shall be seamlessly integrated with the systems engineering process in a cost-effective manner that achieves an optimum balance among opposing mission assurance requirements and between mission assurance requirements versus costs. Figures 8, 9, and 10 provide examples of how the level of efforts of system safety, reliability, and QA programs may be traded off versus system cost incurring characteristics, including prorated loss of system value due to early mission failure.

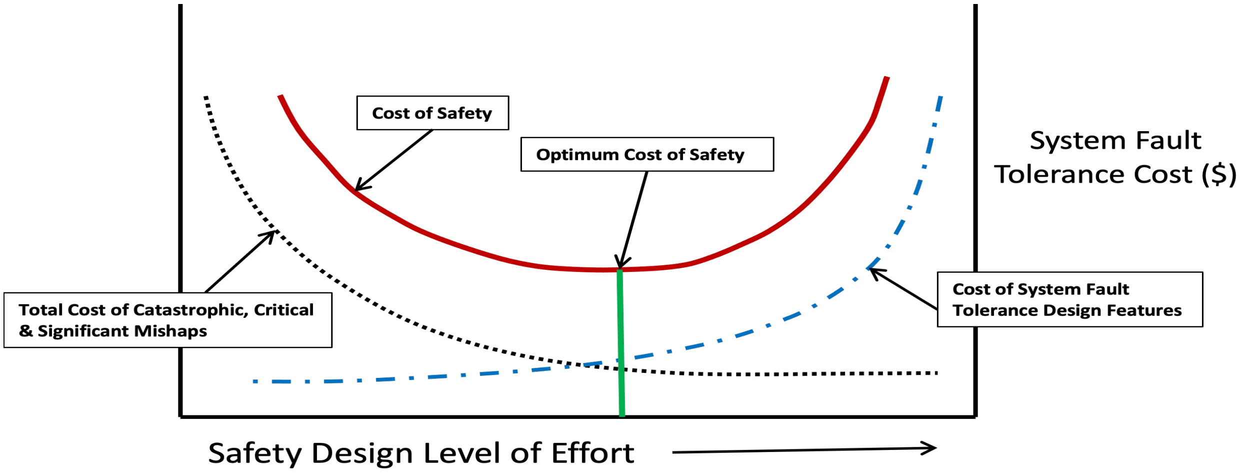


Figure 8: Total Mishap Cost vs. Safety Design Level of Effort.

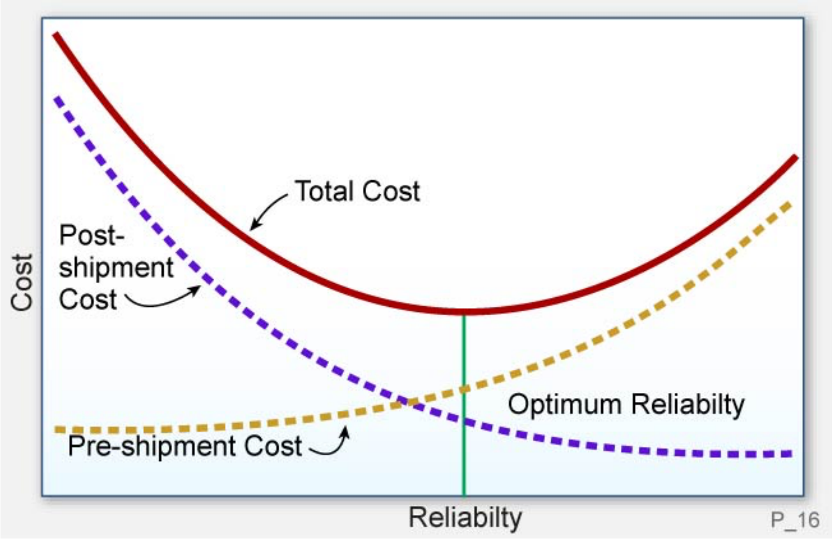


Figure 9: Total System Life Cycle Cost vs. Reliability Design Level of Effort.

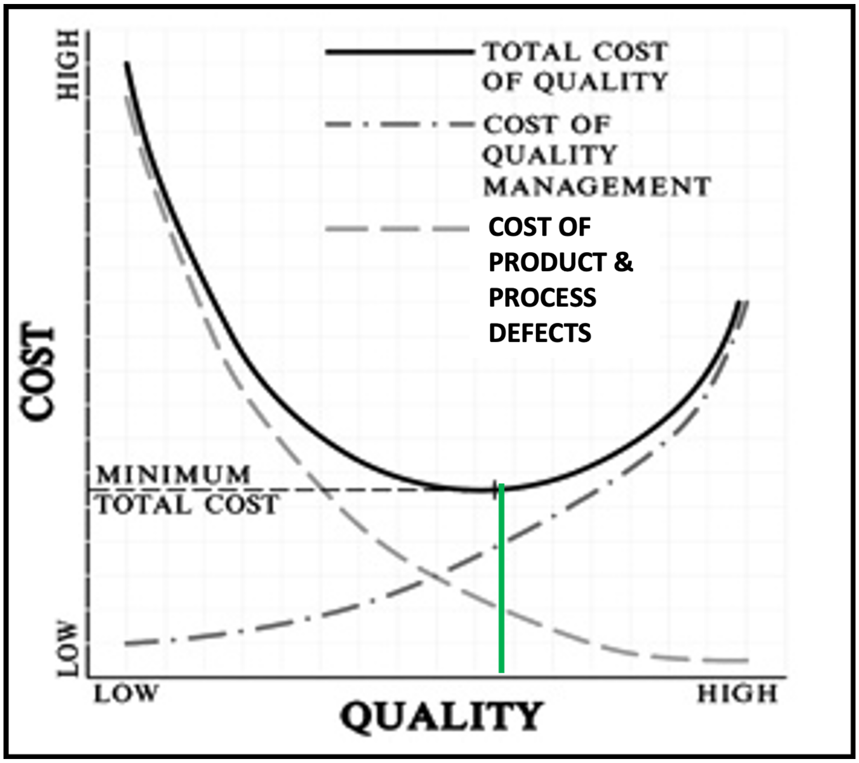


Figure 10: Total Defect Cost vs. Quality Level of Effort.

- SET shall consider the applicability of mission assurance capability level growth commensurate with maturation of the product's development or use when selecting the mission assurance processes. If a Capability Level 2 or above MAP process is required, SET shall document descriptions of the selected processes in approved mission assurance program plans.
- The following factors shall be considered, at a minimum, in the selection of mission assurance process activities:

  1. Unit-value criticality of the end product based on the product unit-value criticality categorizations[3] defined in Annex D (or provide rationale for placing a particular class of product in a different unit-value criticality category);
  2. Applicable systems engineering life cycle phases;
  3. Types of input data available for mission assurance processes;
  4. Applicability of capability level growth, with respect to maturation of the mission assurance input data commensurate with progression of the product development life cycle;

[3] The ordering of generic products according to five unit-value tiers was based on the collective engineering judgment of the S-102 Working Group.

5. Applicable mission assurance design requirements in accordance with the following S-102 prioritized order of importance:
    a. Safety-critical
    b. Mission-critical
    c. Reliability-critical
    d. Maintenance-critical
    e. Monitoring-critical

(Note, deviations from the S-102 prioritized list of design requirements shall be explained in the applicable mission assurance program plan.)

6. Types of product deficiencies addressed by mission assurance processes;
7. Assessed capability of mission assurance processes to achieve specific mission assurance requirements;
8. Capability of mission assurance processes to be integrated cost-effectively with the program's systems engineering process.

5.3.3 Identify the Mission Assurance Guidance Sources

If a Capability Level 2 or higher MAP is required, SET shall identify the documents used as guidance for the Mission Assurance Program, including industry standards and enterprise-level command media. Other sources of guidance include, "Best Practices" and design rules which are recommended by a Standards Development Organization (SDO), and technical papers published by engineering experts.

5.3.4 Establish the Technical Performance Metrics

If a Capability Level 2 or higher MAP is required, SET shall establish Technical Performance Metrics (TPMs) for the purpose of tracking and reporting the progress of each Mission Assurance Program process.

5.4 Coordinate the Mission Assurance Processes with Other Systems Engineering Processes

The MAP manager or his/her representative shall participate in program design reviews, technical interchange meetings, management status reviews, working group meetings, and any other meetings held by the program that may be germane to system safety, RMAD, or Quality Assurance.

5.4.1 Oversee Subcontractor's Mission Assurance Activities

SET shall oversee the Mission Assurance activities of subcontractors during product manufacture, test, inspection, and shipping. If a Capability Level 3 or higher MAP is required, SET shall require major subcontractors to provide mission assurance data products in predefined formats that facilitate integrating these data products with assembly, subsystem, or system level analyses, tests, or inspections.

5.4.2 Establish, Utilize, and Maintain a Project Mission Assurance Database System

If a Capability Level 3 or higher MAP is required, SET shall establish, utilize, and maintain an integrated program-wide Mission Assurance Database System (MADS) that: (1) provides seamless interfaces among mission assurance processes and systems engineering disciplines, such as, Design, Manufacturing, and Test; (2) contains all the key mission assurance requirements and data products; (3) has data change control and tracking procedures; (4) can automatically generate Mission Assurance Program plans and reports that are commensurate with the end product's unit value/criticality, systems engineering process, and applications, and (5) can automatically evaluate Mission Assurance Program plans and reports with regard to measure of compliance with requirements and appropriateness of verification artifacts.

SET shall assure timely utilization of the MADS to the greatest extent practical by Systems engineering disciplines, such as, Design, Manufacturing, Test, and Risk Management. The MADS shall aid in coordinating the assessment of broad categories of system deficiencies as part of the overall Mission Assurance effort. The exchange of mission assurance data products among Systems engineering disciplines shall be governed by approved systems engineering data flow plans. SET shall make every effort to avoid duplication of effort whenever possible.

If a Capability Level 4 or higher MAP is required, all data that are entered in or extracted from the Project Mission Assurance Database System shall be referenced with one or more keyword data element descriptions (DED) listed in Annex C. Each keyword DED belongs to one of the following data types:

- Physical or Functional Characteristic
- Physical or Functional Dependency
- Application
- Failure Mode and Effects Analysis (FMEA) / Hazard Analysis
- Criticality Analysis[4]
- Anomaly Detection, Isolation and Response (ADR)
- Safety, Reliability, or Maintainability Critical Item
- Failure / Hazard Compensation
- Identification
- Unit
- Reference

[4] Hazard rate data, constant failure rate data, and probability of occurrence data all fall under Criticality Analysis DEDs.

- Event
- Diagnostic
- Value
- Comment
- Attachment
- Database Administration

5.5 Apply Engineering and Evaluation Methods to Identify System and Process Deficiencies

SET shall apply validated engineering and evaluation principles and techniques to identify existing and potential system and process deficiencies, including unacceptable design weaknesses as defined in section 5.3.1. SET shall also identify practical methods for avoiding, eliminating, or controlling unacceptable design weaknesses, and for verifying that the implemented mitigation/disposition methods are successful.

The prerequisite for performing a thorough and accurate failure mode, effects, and criticality analysis, or hazard analysis (FMECA/Hazard Analysis), is to first understand how the system operates and its mission success criteria. SET shall ensure that the project's SR&QA engineers are provided with detailed and comprehensive functional diagram models of the system at all indenture levels of the system.

SET and customer shall mutually establish the unacceptable design criteria. The unacceptable design criteria shall be based on studies, analyses, historical data, and test data. The MAP shall use these criteria to further evaluate requirements and designs to see if they are acceptable.

5.5.1 Define the System Failure Criteria and Identify Failure Modes

SET shall define the system failure criteria. If a Capability Level 2 or above MAP process is required, SET shall document the failure criteria in the mission assurance program plan. A severity category shall be assigned to each identified failure mode or hazard based on the worst case end effects on the system or mission, and the probability of occurrence shall be estimated as either a quantitative or qualitative value. Qualitative probability values shall follow the same ground rules as qualitative severity categories. They shall be defined in sufficient detail to allow different people to independently arrive at the same conclusion when reviewing the same data. The definitions in Table 2, for failure mode severity and probability of occurrence categories, shall be used in all mission assurance analyses, evaluations, and tests.

In the absence of a quantitative probability of occurrence analysis, the selection of a qualitative probability value that is based solely on an engineering judgment or guess may be necessary. For all cases where engineering judgment is used in high or serious residual risk acceptance decisions, the source(s) of the engineering judgment shall be identified and verified to have several years of experience in performing detailed reliability predictions on systems, equipment, or processes similar to the one being assessed.

Table 2. Failure Mode Severity and Probability of Occurrence Category Definitions

Value/ Level	Occurrence		Severity		
	Reliability Definitions	System Safety Definitions	Reliability Definitions		System Safety Definitions
5	Very High (1 in 10 or greater)	(A) FREQUENT (X > 10^-1)	1 - Complete loss of mission: complete loss of primary mission capability.		I - 1 - CATASTROPHIC Death, system loss, or severe environmental damage.
4	High (less than 1 in 10 but greater than 1 in 20)	(B) PROBABLE (10^-1 > X > 10^-2)	2 - Major loss or degradation of the primary mission: capability to complete some mission objectives (or all at a degraded level) with immediate loss of a critical science instrument; or loss of a major amount of critical science data; or major reduction in life of the primary mission; or loss of spacecraft function resulting in loss of opportunity for obtaining critical science data.		II - 2 - CRITICAL Severe injury, severe occupational illness, major system or environmental damage.
3	Moderate (less than 1 in 20 but greater than 1 in 100)	(C) OCCASIONAL (10^-2 > X > 10^-3)	3 - Minor loss or degradation of the primary mission: minor loss of spacecraft or instrument function leading to loss of a minor amount of critical science data; or a significant reduction in life of the primary mission; or loss or major degradation of an ancillary mission.	1R - Loss or degradation of a redundant subsystem or science instrument producing level 5 severity, if remaining redundancy is lost.	III - 3 - MARGINAL / SIGNIFICANT Minor injury, minor occupational illness, or minor system or environmental damage.
2	Low (less than 1 in 100 but greater than 1 in 500)	(D) REMOTE (10^-3 > X > 10^-6)	4 - Potential for less than minor loss or degradation of spacecraft or performance: no immediate impact on spacecraft or primary mission, but potential exists for future loss, at severity levels 3 to 5, due to induced failure or resulting from the conjunction of this anomaly with a future event; or potential for cumulative major loss of a mission-critical function over a long period of time; or spacecraft or primary mission loss or significant degradation, at severity level 4, would occur if adequate redundancy, alternatives, or compensating measures are not implemented; or minor degradation of an ancillary mission.	2R - Loss or degradation of a redundant subsystem or science instrument, producing a level 4 severity, if remaining redundancy is lost.	IV - 4 - NEGLIGIBLE Less than minor injury, occupational illness, or less than minor system or environmental damage.
1	Very Low (less than 1 in 500)	(E) IMPROBABLE / NON-CREDIBLE (10^-6 > X)	5 - Insignificant or no impact on spacecraft life or performance: barely noticeable or no performance degradation, and fault does not lead to loss or degradation of instrument data; or loss of significant amount ofancillary mission data; or significant peril to spacecraft or primary mission, at severity level 3, would occur if adequate redundancy, alternatives, or compensating measures are not implemented; or less than minor degradation of an ancillary mission.	3R - Loss or degradation of a redundant subsystem or science instrument, producing a level 3 severity, if remaining redundancy is lost.	V - 5 - NONE / INSIGNIFICANT Failure modes that would have no loss or effects to mission objectives or the environment, or no injuries.

5.5.2 Perform Structured Evaluations

If a Capability Level 5 or higher MAP is required, SET shall develop and apply a structured review process (e.g., a formal peer review working group) to aid thorough evaluation of the MAP's output artifacts in all product life cycle phases. The review process shall include personnel who are cognizant of events that led to failures in systems similar to the one being developed. Product-based and process-based lessons learned that are relevant to the system being developed shall be gathered across the enterprise and used to develop review checklists that support timely implementation of the structured review process and updating of the Mission Assurance Program. The review checklists shall reflect the technical knowledge, insights, design rules, application data, and other clues that helped uncover latent deficiencies. The types of systems engineering artifacts that should be independently reviewed shall include, but are not limited to, those listed in Table 3.

Table 3: Sample Systems Engineering Artifacts

NAME OF DOCUMENT	ARTIFACT CATEGORY
Anomaly Detection and Resolution (ADR) Design Description	Engineering & Evaluation
Approved Parts & Materials List (APML)	Program Coordination
Command Media (Contractor's Internal Practices)	Program Authorization
Critical Item List (CIL)	Engineering & Evaluation
Engineering Memorandum	Engineering & Evaluation
Environmental Analysis Data Report	Engineering & Evaluation
Disposal Plan	Planning
Failure Mode, Effects and Criticality Analysis (FMECA)	Engineering & Evaluation
Fault Tree Analysis (FTA)	Engineering & Evaluation
Failure Report	Engineering & Evaluation
FRACAS Plan	Planning
Hazard Report (HR)	Engineering & Evaluation
Hazard Risk Assessment Matrix (HRAM)	Risk Tracking
Hazardous Material Management Program (HMMP) Report	Planning
Indentured Parts List	Program Coordination
Integrated Master Plan (IMP)	Planning
Integrated Master Schedule (IMS) (Contractor's SR&QA Programs)	Planning
Mishap Investigation Plan (MIP)	Planning
Mishap Risk Assessment Report (MRAR)	Engineering & Evaluation
Missile System Pre-launch Safety Packages (MSPSP)	Engineering & Evaluation
NEPA Facilitation Report	Engineering & Evaluation
On-orbit Operations Handbook (OOH)	Program Coordination
Operational Dependability Analysis	Engineering & Evaluation

NAME OF DOCUMENT	ARTIFACT CATEGORY
Part Stress Derating Analysis	Engineering & Evaluation
Parts, Materials, and Processes (PMP) Program Plan	Planning
Preliminary Hazard Analysis (PHA)	Engineering & Evaluation
Preliminary Hazard List (PHL)	Engineering & Evaluation
Quality Assurance (QA) Program Plan	Planning
Reliability Life Test Plan	Planning
Request for Proposal	Requirements
Risk Management/Mitigation Process Plan	Planning
RMAD Analysis/Assessment Report	Engineering & Evaluation
RMAD Plan	Planning
Safety Assessment Report (SAR)	Engineering & Evaluation
Space Vehicle Survivability Analysis	Engineering & Evaluation
Statement of Work (SOW)	Requirements
Subsystem Hazard Analysis (SSHA)	Engineering & Evaluation
System Hazard Analysis (SHA)	Engineering & Evaluation
System Reliability Assessment Report	Engineering & Evaluation
SR&QA Lessons Learned	Program Coordination
SR&QA Program Plan	Planning
SR&QA Status Report	Program Coordination
SR&QA Working Group Meeting Agenda/Briefing Charts/Minutes/Action Items	Program Coordination
System Specification	Program Coordination
Systems Engineering Management Plan (SEMP)	Planning
System Safety Program Plan	Planning
Test Plan	Planning
Test Report	Verification
Waivers	Risk Tracking

5.5.3 Apply Lessons Learned

If a Capability Level 3 or higher MAP is required, SET shall describe how existing mission assurance data/reports will be reviewed for applicable product-based[5] and process-based[6] lessons learned. Existing lessons learned shall be reviewed to identify possible deficiencies or needed process improvements, such as, improved procedures or training materials.

Candidate lessons learned shall be evaluated for quality, prioritized, and forwarded to the Lessons Learned Approval Authority for appropriate action. SET shall take steps to ensure that candidate lessons learned are documented and reviewed in a timely manner, and the related recommendations infused throughout the project, the stakeholder organizations, and as necessary, enterprise-wide using the appropriate systems. The Project Mission Assurance Database System shall include a field that permits an authorized person to indicate that particular data is a lessons learned candidate. A positive indication in the lessons learned field shall generate a notification to a Lessons Learned Review Committee or similar approval authority regarding the data's candidacy.

If a Capability Level 4 or higher MAP is required, SET shall describe how mission assurance lessons learned will be exchanged with other projects throughout the enterprise, e.g., the project will transmit approved mission assurance lessons learned to other projects for information and comments.

If a Capability Level 5 MAP is required, SET shall describe how non-proprietary lessons learned data will be exchanged with other organizations, e.g., the enterprise will enter into data exchange agreements and employ safeguards to protect security-classified, International Traffic in Arms Regulations (ITAR)-restricted, proprietary, or other sensitive data. The received data will be reviewed by an enterprise-level Lessons Learned Board to identify significant findings that should be implemented on a project or enterprise-wide.

5.5.4 Assess Maturity of Key Input Data, Constraints, Ground Rules, and Analytical Assumptions

If a Capability Level 4 or higher MAP is required, SET shall identify each key input data and its known/anticipated sources, and describe how the maturity of key input data, such as, analytical assumptions, constraints, and ground rules used in the performance of mission assurance processes, will be assessed in accordance with the Table 4 criteria.

Table 4: Key Input Data, Constraints, Ground Rules, and Analytical Assumptions Maturity Ratings

[5] For this standard, a product-based lesson learned is important information created, documented, and retrieved according to a system or device life cycle specific functional or physical descriptor.

[6] For this standard, process-based lesson learned is important information created, documented, and retrieved according to a process or procedure descriptor.

HIGH	**MEDIUM -to-HIGH**	**MEDIUM**	**LOW-to-MEDIUM**	**NEGLIGIBLE–to-LOW**
Based on statistically significant field data	Based on statistically significant test data	Based on simulation model	Based on extrapolated field or test data	Based on engineering judgment or guess

5.6 Risk Assessment and Control

5.6.1 Integrate MAP with Program-wide Risk Management Process

SET shall integrate the mission assurance processes with the program-wide risk management process. Each identified unacceptable risk shall be analyzed, and mitigated or controlled and tracked throughout the systems engineering life cycle. SR&QA risks shall be assessed in respect to severity of effects and likelihood of occurrence. All high and serious residual risks shall be accepted by the appropriate authority. At a minimum, risk mitigation activities shall include:

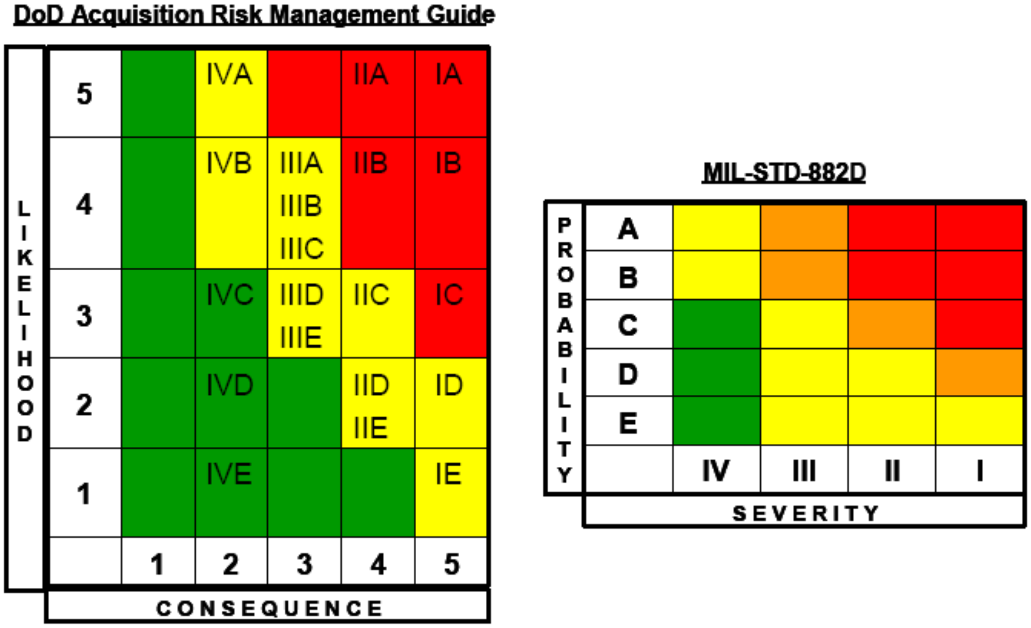
- Establishing the minimum qualifications required to perform each mission assurance process;
- Identifying and reporting instances of significant residual risk to management;
- Managing safety-critical and mission-critical items;
- Monitoring the mission assurance processes to ensure they are performed in accordance with the Integrated Master Schedule (IMS) and the project budget;
- Determining the appropriate responses to unplanned events for each mission assurance process.

In selecting specific fault mitigation or control methods, SET shall apply the following fault disposition method order of precedence. The order in which different methods shall be considered in the disposition of unacceptable faults shall be the following:

- Eliminate faults through design selection. Ideally, the risk of a failure mode should be eliminated. This elimination is often accomplished by selecting a design alternative that removes the fault altogether;
- Reduce risk through design alteration. If the risk of a failure mode cannot be eliminated by adopting an alternative design or alternative material, consider design changes that reduce the severity and/or the probability of a failure mode;
- Incorporate engineered features or devices. If the risk of a failure mode is unable to be eliminated or adequately mitigated through a design alteration, reduce the risk using an engineered feature or device. In general, engineered features actively interrupt the failure mechanism sequence and devices reduce the risk of a failure mode;

- Provide warning devices. If engineered features and devices do not adequately lower the risk of the failure mode, include a detection and warning system to alert personnel to the presence of a faulty condition or occurrence of a undesirable latent event.
- Develop procedures and training. Where other risk reduction methods cannot adequately mitigate the risk from a failure mode, incorporate special procedures and training. Procedures may prescribe the collection of diagnostics or prognostics data. Warnings, cautions, and other written advisories shall not be used as the only risk reduction method for high and serious initial risk levels.

SET shall use the 5x5 risk matrix to assess mission assurance risks. SET shall present all high and serious hazard risks identified using the MIL-STD-882 system safety methodology in the format of the translation table shown in Figure 11.



DoD Acquisition Risk Management Guide

LIKELIHOOD					
5	🟩	🟨 IVA	🟥	🟥 IIA	🟥 IA
4	🟩	🟨 IVB	🟨 IIIA IIIB IIIC	🟥 IIB	🟥 IB
3	🟩	🟩 IVC	🟨 IIID IIIE	🟨 IIC	🟥 IC
2	🟩	🟩 IVD	🟩	🟨 IID IIE	🟨 ID
1	🟩	🟩 IVE	🟩	🟩	🟨 IE
CONSEQUENCE	1	2	3	4	5

MIL-STD-882D

PROBABILITY				
A	🟨	🟧	🟥	🟥
B	🟨	🟧	🟥	🟥
C	🟩	🟨	🟧	🟥
D	🟩	🟨	🟨	🟧
E	🟩	🟨	🟨	🟨
SEVERITY	IV	III	II	I

Figure 11: Translation of MIL-STD-882D Risk Matrix to the OSD Risk Management Guide Matrix

5.7 Verify Mission Assurance Requirements Are Met

5.7.1 Requirements Verification

SET shall verify that each system specification requirement has a corresponding Requirement Verification Plan (RVP) and Requirements Verification Reports (RVR). The Plan of each systems engineering discipline should identify the applicable RVPs and RVRs. The RVPs and RVRs should be entered and maintained in the project-wide Systems Engineering Database.

5.7.2 Verify Use of Industry Acknowledged Engineering Methods

SET shall verify industry acknowledged methods were use by systems engineering disciplines to perform their analytical/engineering related tasks. The engineering reports generated by these disciplines should include references to public domain documents that describe the basis for industry acknowledgement of the systems engineering methods used.

6. ANNEX A

AIAA S-102 Document Tree (normative)

S-102.0.1 Capability-Based Mission Assurance Program General Requirements

Capability-Based MAP Management Requirements

S-102.1.1	Mission Assurance Program(s) Planning
S-102.1.2	Subcontractor and Supplier Mission Assurance Management
S-102.1.3	Mission Assurance Working Group(s)
S-102.1.4	Failure Reporting, Analysis, and Corrective Action System
S-102.1.5	Failure Review Board
S-102.1.6	Critical Item Risk Management
S-102.1.7	Project Mission Assurance Database System
S-102.1.8	Quality Assurance
S-102.1.9	Configuration Management
S-102.1.10	Environmental Safety Assurance

Capability-Based MAP Engineering and Analysis Requirements

S-102.2.1	Functional Diagram Modeling
S-102.2.2	System Reliability Modeling
S-102.2.3	Component Reliability Predictions
S-102.2.4	Product Failure Mode, Effects, and Criticality Analysis
S-102.2.5	Sneak Circuit Analysis
S-102.2.6	Design Concern Analysis
S-102.2.7	Finite Element Analysis
S-102.2.8	Worst Case Analysis
S-102.2.9	Human Error Predictions
S-102.2.10	Environmental Event / Survivability Analysis
S-102.2.11	Anomaly, Detection, and Response Analysis
S-102.2.12	Maintainability Predictions
S-102.2.13	Operational Dependability and Availability Modeling
S-102.2.14	Hazard Analysis
S-102.2.15	Software Component Reliability Predictions
S-102.2.16	Process Failure Mode, Effects, and Criticality Analysis
S-102.2.17	Event Tree Analysis
S-102.2.18	Fault Tree Analysis
S-102.2.19	Fishbone Analysis
S-102.2.20	Similarity and Allocations Analysis
S-102.2.21	Component Engineering
S-102.2.22	Stress and Damage Simulation Analysis

Capability-Based MAP Testing Requirements

S-102.3.1	Environmental Stress Screening
S-102.3.2	Reliability Development / Growth Testing
S-102.3.3	Reliability, Maintainability, and Availability Demonstration Testing
S-102.3.4	Reliability Life Testing
S-102.3.5	Design of Experiments
S-102.3.6	Ongoing Reliability Testing (ORT)
S-102.3.7	**Product Safety Testing**

7. ANNEX B

Mission Assurance Program General Requirements (normative)

7.1 The Capability Level 1 Mission Assurance Program shall include the following tasks:

7.1.1 Timely authorization

Timely authorization of the contractor's mission assurance organizations which are assigned the responsibility and authority for meeting the mission assurance requirements and objectives. The following independent programs shall be authorized at a minimum: a System Safety Program, a Reliability, Maintainability, Availability, and Dependability (RMAD) Program, and a Quality Assurance (QA) Program;

Assign qualified management and engineering personnel, and obtain the tools needed to cost-effectively implement the SR&QA programs. These individuals shall use validated methods to identify and eliminate or control of unacceptable deficiencies, as required;

7.1.2 Timely identification

Timely identification of the appropriate quantitative and qualitative mission assurance requirements. These requirements shall be consistent with the system requirements and this Standard, and shall be flowed down to all affiliated subcontractors;

- Timely identification of any mission assurance requirements which may be satisfied by an existing analysis, inspection, test report, or data product from a similar project, product, or process;

7.1.3 Timely selection

In lieu of a formally approved project Mission Assurance Program Plan (MAPP), timely selection of the set of Capability Level 1 Mission Assurance processes which comprise the "baseline" processes of a Mission Assurance Program (MAP) that is tailored to achieve the minimum acceptable level of mission assurance risk. NOTE: This set of "baseline" processes may be defined by the contractor's MAP command media. Identify the input sources, output uses, schedule/milestone tracking, estimated time to complete (ETC) or level of effort (LOE) in hours, and method for managing risk (which includes monitoring, evaluating, reporting, and responding to anticipated and unanticipated problems);

Note: This set of processes constitute the minimum effort required to control specific deficiency risks for a specific life cycle of a low unit-value product. The following factors shall be considered, at a minimum, in the selection of mission assurance processes:

1. Unit-value criticality of the end product based on the product unit-value criticality categorization defined in Annex D;
2. Applicable product life cycle phases;

3. Types of input data available for mission assurance processes;
4. Applicability of capability level growth, with respect to maturation of the mission assurance input data commensurate with progression of the product development life cycle;
5. Applicable mission assurance requirements; in accordance with the S-102 prioritized list of design requirements:
    a. Safety-critical
    b. Mission-critical
    c. Reliability-critical
    d. Maintenance-critical
    e. Monitoring-critical

(Note, deviations from the S-102 prioritized list of design requirements shall be explained in the applicable mission assurance program plan.)

6. Types of product deficiencies addressed by mission assurance processes;
7. Assessed capability of mission assurance processes to achieve specific mission assurance requirements;
8. Capability of mission assurance processes to be integrated cost-effectively with the project's systems engineering process.

7.1.4 Timely coordination

Timely coordination of mission assurance activities with other functions in the project's systems engineering process;

NOTE: Coordinate the interactions required for successful implementation of each mission assurance process,

7.1.5 Timely implementation of processes

Timely implementation of the selected engineering and evaluation processes;

a. Timely review of detailed and comprehensive functional diagram models of the system;
b. Timely definition of the system failure criteria;
c. Timely identification of system failure modes and their qualitative probability of occurrence.

7.1.6 Timely implementation of product risk management principles

7.1.7 Timely definition

Timely definition of the formal and informal methods which will be used to verify the mission assurance requirements are met. The formal verification methods shall involve review and concurrence by the acquisition authority. Product Safety Testing shall be performed in a formal manner. The informal verification methods shall involve review and concurrence by internal management only;

7.1.8 Timely documentation

Timely documentation of the MAP results in safety, reliability, and quality assurance (SR&QA) assessment reports, as required, and distribution of those reports to the acquisition authority. The SR&QA assessment reports shall be updated on an "as required" or "as needed" basis. An "as required" update would be triggered by scheduled events which include contractually required delivery frequency, and an "as needed" update would be triggered by unscheduled events which include the availability of better input data for the assessment.

7.2 The Capability Level 2 Mission Assurance Program shall include all the tasks in the Capability Level 1 Mission Assurance Program plus the following at a minimum:

7.2.1 Change

Change 8.1.5 to, "Timely selection and implementation of the set of Capability Level 2 Mission Assurance processes which comprise the minimum effort required to control specific deficiency risks for a specific life cycle of a medium unit-value product. The following factors shall be considered, at a minimum, in the selection of mission assurance processes:"

7.2.2 Timely establishment

Timely establishment of a formal approval process for the Mission Assurance Program Plan (MAPP), which includes review and concurrence by internal managers and the acquisition authority;

7.2.3 Timely documentation

Timely documentation, approval, flow down (as appropriate) and implementation of a MAP plan that is an integral part of the Systems Engineering Plan (SEP). The MAP plan establishes the organization, responsibilities, objectives, and approach of the Mission Assurance Program, including the following at a minimum:

- Establishment of Mission Assurance Program organization(s);
- Establishment of Mission Assurance implementation responsibilities, authority and accountability;
- Establishment of program-wide Mission Assurance requirements;
- Establishment of standards, guides, or enterprise-level command media that govern the Mission Assurance Program(s);

Note: The MAP plans shall be updated on an as required or as needed basis. As required updates include contractually required delivery frequency and as needed updates include incorporating better data.

7.2.4 Timely establishment

Timely establishment of Technical Performance Metrics for purposes of tracking and reporting the progress of each Mission Assurance Program process.

7.2.5 Timely oversight

Timely oversight of the Mission Assurance activities of subcontractors during product manufacture, test, inspection, or shipping.

7.2.6 Change

Change B.1.5c to "Timely identification of system failure modes and their quantitative probability of occurrence."

7.3 The Capability Level 3 Mission Assurance Program shall include all the tasks in the Capability Level 2 Mission Assurance Program plus the following:

7.3.1 Change

Change B.2.1 to, "Selection and implementation of the set of Capability Level 3 Mission Assurance processes which comprise the minimum effort required to control specific deficiency risks for a specific life cycle of a high unit-value product. The following factors shall be considered, at a minimum, in the selection of mission assurance processes"

7.3.2 Establish, utilize, and maintain

Establish, utilize, and maintain a project Mission Assurance database system that: (1) provides seamless interfaces among mission assurance processes and systems engineering disciplines, such as, Design, Manufacturing, and Test, (2) contains all the key mission assurance requirements and data products, (3) has data change control and tracking procedures; and (4) can generate Mission Assurance Program plans and reports that are commensurate with the end product's unit value/criticality, systems engineering process, and application; (4) can automatically generate Mission Assurance Program plans and reports that are commensurate with the end product's unit value/criticality, systems engineering process, and applications, and (5) can automatically evaluate Mission Assurance Program plans and reports with regard to measure of compliance with requirements and appropriateness of verification artifacts.

7.3.3 Assure

Assure other project functions utilize Mission Assurance results/data to the greatest extent practical.

7.3.4 Collect, review, and utilize

Collect, review, and utilize existing Mission Assurance lessons learned, as applicable;

7.3.5 Evaluate

Evaluate all aspects of the Mission Assurance Program to identify and approve new product and process based candidate lessons learned.

7.4 The Capability Level 4 Mission Assurance Program shall include all the tasks in the Capability Level 3 Mission Assurance Program plus the following:

7.4.1 Change

Change B.3.1 to, "Selection and implementation of the set of Capability Level 4 Mission Assurance processes which comprise the minimum effort required to control specific deficiency risks for a specific life cycle of a very-high unit-value product. The following factors shall be considered, at a minimum, in the selection of mission assurance processes"

7.4.2 Change

Change B.2.5 to, "Oversee the Mission Assurance activities of subcontractors, such that, major subcontractors provide mission assurance data products in predefined formats that facilitate integrating component level mission assurance data products with assembly, subsystem, or system level analyses, tests, or inspections."

7.4.3 Evaluate

Evaluate the maturity of the mission assurance input data in accordance with the project Risk Management Plan and AIAA S-102.0.1. (e.g., Rate the maturity of key constraints, ground rules, and analytical assumptions used in the performance of each Mission Assurance process);

7.4.4 Acquire

Acquire validated computer-aided tools for each Mission Assurance process, and integrated them to form a comprehensive computer-aided Mission Assurance toolset, to the greatest extent practical.

7.4.5 Develop and maintain

Develop and maintain a program-wide Mission Assurance database that complies with the AIAA S-102 Mission Assurance data element description (DED) requirements;

7.4.6 Establish channels

Establish channels to exchange approved lessons learned with similar projects throughout the enterprise;

7.4.7 Integrate

Integrate all mission assurance risk assessments with a single program-wide Risk Management Process to assure that all risks associated with hazards, failure modes, or defects are properly addressed, and that any residual risks are reported to the customer in a timely manner. At a minimum, this approach shall include the following activities:

a. Establishing minimum qualifications to minimize risk associated with experience-intensive or training-intensive activities;

b. Identifying and reporting instances of significant residual risk to project management;

c. Managing safety-critical and mission-critical items;

d. Monitoring the mission assurance processes to ensure they are performed in accordance with the Integrated Master Schedule (IMS) and the project's budget;

e. Deducing ways of avoiding anticipated unplanned events that may affect the product's safety/reliability design, or the project's schedule/budget,

f. Responding appropriately to unplanned events that affect the product's safety/reliability design, or the project's schedule/budget.

7.5 The Capability Level 5 Mission Assurance Program shall include all the tasks in the Capability Level 4 Mission Assurance Program plus the following:

7.5.1 Change

Change B.4.1 to, "Selection and implementation of the set of Capability Level 5 Mission Assurance processes which comprise the minimum effort required to control specific deficiency risks for a specific life cycle of a ultra-high unit-value product. The following factors shall be considered, at a minimum, in the selection of mission assurance processes"

7.5.2 Perform formal peer reviews

Perform formal peer reviews to evaluate the Mission Assurance Program outputs;

7.5.3 Continuously improve

Continuously improve all Mission Assurance Programs by;

- Instituting procedures to facilitate the proactive identification and implementation of needed improvements in mission assurance processes (e.g., conduct surveys to quantify the value of documented results as perceived by independent professionals, internal and external organizations, and other projects.);
- Periodically train the appropriate management and engineering personnel in the use of mission assurance tools and the cost-effective implementation of mission assurance processes;
- Integrating mission assurance lessons learned into the training materials.

7.5.4 Share lessons

Share approved Mission Assurance lessons learned with external enterprises and organizations.

8. ANNEX C

MISSION ASSURANCE PROGRAM DOMAIN DESCRIPTIONS

8.1 SYSTEM SAFETY PROGRAM

The contractor shall assign a system safety manager to implement the system safety requirements of the program commensurate with the contractual requirements. The system safety manager shall be responsible for the establishment, control, incorporation, direction and implementation of the system safety program and assuring that hazard risk is identified, eliminated, or controlled within established program risk acceptability parameters. The system safety manager shall establish internal reporting procedures for the investigation and disposition of product related hazards and safety incidents, including potentially hazardous conditions not yet involved in a mishap/incident. Such matters require timely reporting to the program manager and customer, as required.

8.2 System Safety Management Tasks

8.2.1 System Safety Program Planning

Purpose: To identify the activities essential in assuring the System Safety tasks required to identify, evaluate, and eliminate or control hazards, or to reduce the residual hazard risk to a level acceptable throughout the system life cycle. The approved System Safety Program Plan (SSPP) demonstrates that the program manager fully understands his/her system safety obligations to the customer and to the Contractor, and that the resources necessary to fulfill this obligation are allocated. For the customer, the SSPP provides the means for understanding how the program accomplishes its system safety responsibilities, as called out in the program statement of work (SOW) or this Standard.

Process Description: The System Safety Program Plan (SSPP) assures safety design risks are balanced against project constraints and objectives through a comprehensive effort that will contribute to system safety over the product life cycle. The SSPP is developed as part of the initial planning for all product development programs. The SSPP shall include descriptions of the following:

a. The responsibilities of the system safety organization

b. The system safety responsibilities of key individuals and organizations outside the system safety organization

c. How the system safety program will be established and implemented consistent with contractual requirements

d. How system safety standards and guidance will be provided to all program disciplines consistent with contractual requirements

e. The single Point of Contact for all system safety matters pertaining to the program, the customer, the subcontractors, and the Contractor

f. How all reasonable and prudent hazard risks will be assessed, and eliminated, controlled, or accepted during all phases of the program

g. How the flow down of system safety requirements to subcontractors will be consistent with contractual requirements

h. How product and operational safety issues will be brought to the attention of the program manager in a timely manner

i. How the generation and delivery of system safety documents, and other items related to system safety contractual deliverables, will be consistent with contractual requirements

j. How system safety engineers will participate in technical reviews, design change reviews, and trade studies to ensure compliance with applicable system safety requirements

k. How system safety audits and reviews, if contractually required, will be conducted to ensure compliance with system safety policies, procedures, and functional performance requirements

l. How the resources needed to accomplish the system safety program tasks will be assured.

8.2.2 Subcontractor & Supplier System Safety Management

Purpose: To identify sources of products and services that may be used to satisfy system safety requirements, and manage the pertinent activities of subcontractors and suppliers to minimize risk of hazardous conditions. Also, to assure system safety activities of subcontractors are consistent with the overall system safety program through verification of compliance or conducting surveillance of their system safety activities.

Process Description: Exercise monitoring and control of subcontractor and supplier system safety activities; assure system safety program plans are complete and executable; exchange applicable system safety lessons learned; and if necessary, assist in development of their system safety capabilities. All system safety deliverables expected from the subcontractor shall be called out in contractual agreements with the subcontractor.

8.2.3 System Safety Program Working Group

Purpose: To conduct formal and informal technical reviews, determine the status of a system safety program, and work system safety risks and issues to closure.

Process Description: System safety engineers meet to review status of planned system safety activities, significant hazard risks, and any mishaps which may have occurred. The group also assures appropriate follow-up actions or corrective actions are taken in a timely manner, and are properly implemented, verified, and documented.

8.3 System Safety Engineering Tasks

8.3.1 Hazard Analysis

Purpose: To identify hazardous conditions and risks for purpose of elimination and/or control. Hazard analysis is performed to examine the system, subsystems, components, and their interrelationships, as well as logistic support, training, maintenance, operational environments, and system/component disposal plans to:

a. Identify hazards and recommend appropriate corrective action.

b. Assist the individual(s) actually performing the analysis in evaluating the safety aspects of a given system or element.

c. Provide managers, designers, test planners, and other decision makers with the information and data needed to permit effective tradeoffs.

d. Demonstrate compliance with given safety-related technical specifications, operational requirements, and design objectives.

Process Description: The timely identification of unacceptable hazards is the first activity in assuring proper safety provisions. Identification involves determining the severity or magnitude, importance, and frequency or likelihood of the worst-case mishap caused by the hazard at every system indenture level. Timely evaluation of unacceptable hazards involves determining the appropriate corrective action to eliminate or control unacceptable hazards and avoid the postulated mishaps of catastrophic or critical severity. Timely communication of the hazard evaluation results to individuals with decision-making authority to implement corrective actions. Needed safety design changes should be identified and completed early in the system's life cycle to minimize the impact on cost and schedule.

8.3.2 Fault Tree Analysis

Purpose: To systematically examine a potential system failure by creating a graphical representation of the system using deductive logic. The fault tree represents system relationships and fault paths, and provides a means for qualitative or quantitative system evaluation. Fault tree analysis (FTA) is a deductive, top-down method used to determine how a given system failure can occur. A system's top undesired event is either identified or postulated, and the analysis attempts to find out what contributes to this undesirable event.

Process Description: The FTA begins with a top event, establishes the component-level to which each system-level fault is examined, and determines the immediate causes for each fault at progressively lower levels until a component-level fault is reached. The FTA determines the various ways in which a particular type of top event or failure could occur. All of the possible system contributing factors and their relationships shall be established and, if possible, a top probability of occurrence calculated.

The primary output of FTA is the fault tree structure, which allows for qualitative or quantitative evaluation of a system failure. FTA is particularly useful in the examination of functional paths of high complexity, in which the outcome of one or more combinations of non-critical basic events may produce an undesirable system failure. Typical candidates for FTA are functional paths or interfaces that could have impact on flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error-free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. Fault tree is an analysis tool that provides a way to combine all contributing failures, events, and conditions that can lead to the occurrence of an undesired top event.

8.3.3 Event Tree Analysis

Purpose: To systematically examine various possible outcomes of a given initiating event and create a graphical model of the system logic. The event tree represents system relationships and accident paths and provides a means for qualitative or quantitative system evaluation. Event Tree Analysis (ETA) is an inductive process that shows all possible outcomes (end states) resulting from an initiating event, and can expand accidental events into scenarios that take into account all safety mitigation measures whether functioning or not and additional factors impacting the outcomes.

ETA can be used to identify all possible accident scenarios and sequences of events in a complex system allowing for identification of the system's design and operational weaknesses. This can lead to improvements in system safety functions and result in lowering the operational risks of technologically advanced systems.

Process Description: ETA is an accident propagation analysis tool. The analysis is conducted in the form of a decision tree and is based on a binary logic distinction between success and failure. It begins with an initiating event (the root of the tree) and follows it through the system to determine a range of its potential outcomes (end states). The logic describes the states in which an event either has or has not occurred or a component has or has not failed. This corresponds to the functions or subsystems and their success or failure of being activated given the existing conditions. Each branch of the ET includes probability of success or failure. Such accident sequences allow using the Boolean logic for quantification of system risks.

The primary output of ETA is the event tree structure, which allows for qualitative or quantitative evaluation of a range of possible accident end states. ETA is particularly useful in the examination of accident propagation paths of highly complex designs, in which the failure of one or more combinations of mitigating events may produce undesirable consequences. Typical candidates for ETA are functional paths or interfaces that could impact flight safety, munitions handling safety, safety of operating and maintenance personnel, and probability of error free command in automated systems in which a multiplicity of redundant and overlapping outputs may be involved. Event tree analysis in combination with fault tree analysis is an analysis tool that provides a way to combine all contributing failures, events, and conditions that can lead to either success or failure of a complex system.

8.3.4 Human Error Predictions

Purpose

To perform user/operator level reliability predictions and assessments based on a critical-function analysis that characterizes human performance capabilities, historical performance data, and operator interfaces with the system design. This task aids in evaluating the reliability of users / operators, and provides key input to system reliability modeling / predictions.

Process Description

Develop a mathematical model to estimate the failure rate or hazard rate of the user / operator. The model shall represent: (1) historical operator error rates versus skill levels, (2) critical-function procedures, (3) error mitigation features, (4) training effectiveness, and (5) a hazard assessment of operator interfaces.

8.3.5 Environmental Safety Assurance

Purpose:

To give appropriate consideration to potential environmental impacts prior to beginning any action that may significantly affect the environment.

Process Description:

The contractor shall implement Environmental Safety Assurance. prior to the start of a construction/demolition project or system deployment/disposal to identify and eliminate or control risk items that can adversely affect the environment, and to reduce the risk of violating federal, state, or local environmental laws/regulations to an acceptable level. When properly implemented, Environmental Safety Assurance has negligible effects on the scheduled development of a system.

8.4 System Safety Testing Tasks

8.4.1 Product Safety Testing (PST)

Purpose:

Tests are defined during the Engineering and Manufacturing Development Phase to validate selected safety features of the system or product. Safety critical equipment is tested to determine mishap severity or to establish the margin of safety of the design.

Process Description:

The contractor shall implement demonstrate the acceptability of safety critical equipment, inducing or simulating failure modes. When it cannot be analytically determined whether the corrective action will adequately control a hazard, safety tests will be conducted to evaluate the effectiveness of the controls. Safety testing shall be integrated into system test and demonstration plans to the maximum extent possible.

9. RELIABILITY, MAINTAINABILITY, AND AVAILABILITY (RMAD) PROGRAM

The contractor shall assign an RMAD manager to implement provisions of the program commensurate with the contractual requirements. The manager is responsible for the establishment, control, incorporation, direction and implementation of the RMAD Program.

9.1 RMAD Management Tasks

9.1.1 RMAD Program Planning

Purpose: To identify those activities and designs essential in assuring product reliability, maintainability, availability and dependability performance.

Process Description: RMAD Program Plan assures reliability, maintainability, availability and dependability risks are balanced against project constraints and objectives through a comprehensive effort that will contribute to system reliability over the mission life cycle. This is performed as part of the initial planning for all product development programs. The RMAD Program Plan includes a description of how each task is implemented in each program phase, including the roles of key participants, and a listing of the key outputs of each task. The Plan encompasses a set of analytical activities that include the development of probabilistic system reliability requirements, the analysis of failure modes and effects, the identification and control of critical/limited life items, the development of probabilistic reliability models, the determination of component/part failure rates, the use of worst-case and parts stress analysis, and the implementation of a failure recurrence prevention system which ensures that all failures are adequately driven to closure.

9.1.2 Subcontractor & Supplier RMAD Management

Purpose: Identify sources of products and services used to satisfy reliability, maintainability, availability and dependability requirements, and manage the pertinent activities of subcontractors and suppliers to minimize risk of latent deficiencies. Assure RMAD activities of the subcontractor or supplier are consistent with the overall RMAD Program, through verification of compliance, or surveillance of their reliability, maintainability, availability and dependability activities.

Process Description: Monitor and control of subcontractor and supplier reliability engineering activities; assure that their reliability program plans are complete and executable; exchange applicable reliability lessons learned; and if necessary, assist in development of their reliability capabilities. All reliability deliverables expected from the subcontractor shall be called out in contractual agreements with the subcontractor.

9.1.3 RMAD Working Group

Purpose: To conduct formal and informal technical reviews, determine the status of the RMAD program, and work reliability, maintainability, availability and dependability risks and issues to closure.

Process Description: Engineers cognizant of the project's RMAD requirements meet to review the status of planned reliability activities, significant failure mode risks, and any verified test failures. The group also assures required follow-up actions or corrective actions are taken in a timely manner, and are properly implemented, verified, and documented.

9.2 RMAD Engineering Tasks

9.2.1 Functional Diagram Modeling (FDM)

Purpose: To develop graphical representations of the system's functional interrelationships. The primary output of FDM is a graphical diagram that represents detailed design information with regard to the functional characteristics of each system element. FDM assists in achieving a common understanding, in a functional sense, of the system or system of systems among all Systems Engineering disciplines. The FDM, also referred to as a Functional Block Diagram (FBD), can be thought of as a "bridge", serving as the link between the technical engineering documentation such as drawings, ICDs, and so forth, to the Failure Mode, Effects and Criticality Analysis (FMECA).

Process Description: Collect, process, and evaluate detailed system design information to develop a graphical representation of the system that consists of:

a. The system's functional elements, including inputs and outputs of each functional element;

b. The system's functional paths (e.g., wiring, tubing, logic flow, operator actions, power, signals, electromagnetic waves, forces, pressures, and mechanical motions)

c. References to a description of the system's modes of operation (e.g., mission timeline, states, transitions, switching, timing, and phases);

9.2.2 Product Failure, Mode, Effects & Criticality Analysis (FMECA)

Purpose: To identify effects of potential failure modes, system redundancy features, responses to system failures, single point failure modes, and critical items which require special controls during processing.

Process Description: An FMEA/FMECA is prepared whenever a system functional block diagram is available, and should be updated throughout the system development cycle. The FMEA/FMECA process is used to identify credible single-point failure modes and feed into the critical items controls process to eliminate or control their effects. See Figure C-1 for a flow depiction for the FMEA/FMECA and CIL Analysis process.

FMEA: Perform a systematic analysis of local and system effects of specific component failure modes.

FMECA: Evaluate mission criticality of each failure mode. Criticality analysis is applied to the design process to eliminate safety critical flaws in the system or mitigate those failures, by actions such as providing redundant features or identifying operator actions which can be taken. Also can be used to identify failures of a less critical nature, but which are determined to be maintainability drivers.

Critical Items List (CIL): Provides a summary of selected hardware related items whose related failure modes can result in serious injury, loss of life (flight or ground personnel), loss of vehicle, or loss of one or more mission objectives.

9.2.3 Component Reliability Predictions

Purpose: To perform part and component level reliability predictions and assessments. This task aids in evaluating the reliability of similar components, and provides key input to system reliability modeling.

Process Description: Develop a mathematical model to estimate the failure rate or hazard rate of the component for a given operating mode, operating cycles, and under specified operating conditions. The model should provide insight into component level redundant functions.

9.2.4 System Reliability Modeling

Purpose: To perform assembly through system level reliability predictions, allocations, and assessments. Aids in evaluating reliability of competing designs, and provides key input to availability and sparing assessments.

Process Description: Develop a hierarchical mathematical model to estimate the probability of the system successfully performing its intended functions for a given period of time or operating cycles, and under specified operating conditions. The model should account for initial system reliability, which includes the cumulative effects of functional testing, storage, handling, packaging, transportation, assembly, and maintenance on the ability of the system to meet its operational reliability requirements. The model should provide insight into assembly through system level redundant functions.

9.2.5 Design Concern Analysis (DCA)

Purpose: To assure a safe and reliable product by designing-in special features that prevent, tolerate, or recover from failures, compensate for potential design weaknesses, or mitigate risk.

Process Description: Design rules and guidelines may be used to upfront to ensure a degree of product durability by avoiding specific types of design weaknesses. Or, perform an analysis on an existing design to identify where special features are needed to mitigate a design weakness. Some of these special features include redundancy, fault tolerance, fail-safe, and design margin.

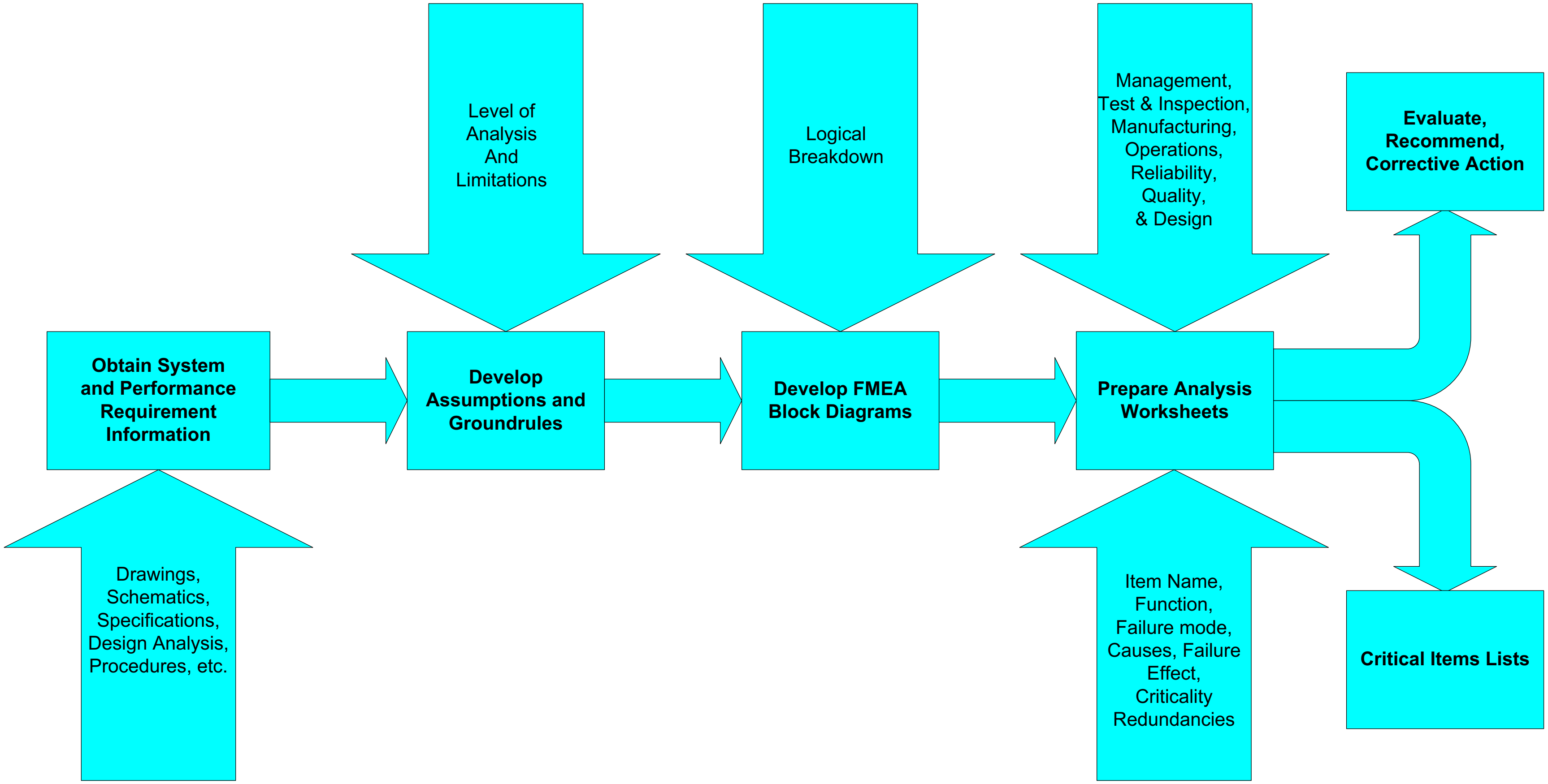


Figure C-1. FMEA/FMECA & CIL Analysis Process.

9.2.6 Worst Case Analysis (WCA)

Purpose: To ensure that all circuits will perform within specifications over a given lifetime while experiencing the worst possible variations of electrical piece parts and environments.

Process Description: During preliminary design, evaluate circuit performance assuming maximum part parameter variations and extreme operating conditions, e.g., long use life, high temperature, radiation, shock, etc.

9.2.7 Environmental Event / Survivability Analysis

Purpose: To ensure the system will physically survive its natural operating environmental by one or more of the following methods:

a. Performing a environmental hazard analysis to verify the probability of environmentally induced damage is non-credible (i.e., < 10^-6),

b. Showing proper electromagnetic interference (EMI) margin exists for all components susceptible to anticipated single event upsets (SEUs),

c. Using commercial products that meet Federal Communications Commission (FCC) or European Union EMC requirements or MIL-STD-461C requirements, and,

d. Showing that system functionality will be restored following the occurrence of environmentally induced damage.

Process Description: Identify environmental hazards and develop a mathematical model to estimate the failure rate or hazard rate associated with environmental event susceptible parts. The model shall represent:

a. Historical failures of similar systems in similar operating environments,

b. Components susceptible to environment induced damage,

c. Environmental damage mitigation features, and,

d. Assessment of the system restoration capability.

9.2.8 Software Component Reliability Predictions

Purpose: To quantify the probability or frequency of a software component's functional success or failure. Predictions are expressed as a statistical life distribution that represents the probability of a software component functioning during a particular time period. This task aids in ensuring software design reliability, and it provides key input to system reliability modeling / predictions.

Process Description: Develop mathematical or simulation models which represent the following software component attributes:

a. Architecture

b. Application

c. Use environment

d. Operating profile

e. Failure modes, mechanisms, and causes

9.2.9 Maintainability Predictions

Purpose: To perform probabilistic estimates of failure maintenance times based on maintenance time-study data, diagnostics capability of the design, and accessibility of failed components. Maintainability predictions are performed to aid:

a. Defining / meeting repair time requirements,

b. Identifying where design features are needed to reduce the repair time, and,

c. Ensuring all repair actions are characterized and repeatable.

The output of maintainability predictions is primarily used to support integrated logistics support (ILS) assessments. This task aids in ensuring maintenance training and skill levels are compatible with system design, and it provides key input to system availability and dependability modeling / predictions.

Process Description: Perform maintainability predictions to support system availability and dependability modeling / predictions, and ILS assessments, as required.

9.2.10 Anomaly Detection and Response (ADR) Analysis

Purpose: To develop identification and response methods for system anomalies or faults which pose an unacceptable risk. Depending on how it is performed, ADR analysis can be used to develop different types of ADR systems. The primary output of ADR analysis are functional failure analysis (FFA) worksheets, which systematically identify the detection and response methods for functional failure modes that require such actions, as defined by FMECA, system tests, test deficiency reports, failure analyses, hazard analyses, or risk assessments.

Process Description: Perform an analysis to design system functions for detecting, verifying, isolating, and responding to a specified set of functional failure modes. The ADR analysis process includes the following tasks:

a. Defining ADR system requirements and design criteria which meet the user’s needs;

b. Establishing ADR analysis technical performance metrics (TPMs);

c. Collecting and evaluating engineering information needed to perform the analysis (e.g., signal lists, specs, interface control drawings (ICDs), test data, operational data, schematics, and product FMECA);

d. Developing functional failure analysis (FFA) worksheets which define the detection, verification, isolation, and response methods, as applicable, for each identified functional failure mode;

e. Validating each FFA worksheet, and;

f. Documenting the ADR analysis.

9.2.11 Operational Dependability and Availability (D_O/A_O) Modeling

Purpose: To develop mathematical or simulation models to be used for probabilistic apportionments or predictions of the percentage of total time or number of system cycles is expected to occur based on the collective R&M characteristics of all the functional items required for a system to successfully perform its mission or be capable of starting its mission. The primary outputs of D_O/A_O modeling are:

A probabilistic assessment that the system will be available for service when required, or that it will successfully complete a mission given its availability at the start of the mission;

A probabilistic assessment that the system will be available for service at a specific instant in time, or that it will in service during a mission at a specific instant in time given its availability at the start of the mission.

Process Description: Operational Dependability and Availability modeling / predictions using as inputs the system's operational reliability characteristics, based on engineering data that reflects the mission environments and system usage, and the system's maintainability characteristics. Input data used to develop mathematical or simulation D_O/A_O models include the following:

a. System hierarchical functional flow

b. System operating modes and the mission timeline

c. Functional to physical association of each item in the system, to include as a minimum:

d. All electrical, electronic, and electromechanical (EEE) and software components that perform essential functions in each specified mission time period or operating cycle, e.g., switches and sensors that control restorable functions

e. All mechanical, pneumatic, pyrotechnical, and structural items that perform essential functions in each specified mission time period or operating cycle

f. System-level effects due to the loss of each functional item in the system

g. Operational failure rate or hazard rate for each software and hardware functional item in the system

h. Operational restoration rate for each functional and physical item in the system. (The restoration rate includes the time to restore the item to full operational functionality from the time the item is first taken out of service, whether due to scheduled or unscheduled maintenance).

i. Logistics delay time to replace each software and hardware replaceable component in the system.

The amount of effort required to develop accurate predictions for system-level D_O/A_O is dependent on the complexity of the system, its mission environment, and its usage.

9.2.12 Similarity and Allocations Analysis

Purpose: To extrapolate the performance of unknown parameters of a product based on an assessment of known parameters of a similar product.

Process Description: Select a sample product that is closely similar to the target product for which knowledge of key performance parameters is desired. Identify the parameters that are similar and dissimilar between the two products. Use the known performance parameters of the sample product to extrapolate the performance parameters of the target product.

9.2.13 Finite Element Analysis

Purpose:

Finite element methodologies are used to:

a. Perform structural stress analysis to identify peak stresses, stress distributions and transmission patterns. This is used to assess the effectiveness of an electronic device's physical packaging to maintain structural and circuit interconnection integrity and a suitable environment for the circuits to function reliably. Analytical evaluations of these physical aspects transform the discipline of electronics packaging from a subjective art into an objective science.

b. Perform thermal stress analysis to determine the response of an electronic device to the thermal stresses anticipated throughout its service life. Thermal analysis predicts the maximum temperature of an electronic module, and the temperature of its individual components, due to internal heating, when subjected to various power and usage loading conditions.

Process Description:

Perform structural stress analysis to study and compute deformations, internal forces, and stresses using an appropriate set of physical laws and mathematics to predict the behavior of structures. The structural analysis process shall incorporate the fields of mechanics and dynamics as well as applicable failure theories.

Electrical stress evaluations shall be performed as part of the electronic analysis process. Physical packaging of electronics involves the ergonomics, mechanical support, electrical connections, power, thermal and environmental management features that sustain the components in an electronic device.

Perform structural stress analysis to:

a. Identify the loading factors that will stress the device in its intended application.

b. Calculate the device's strength and stress-strain relationships transferred throughout the device.

c. Verify that the strain doesn't exceed material yield points, which could cause imminent failure.

d. Identify items that may be highly or frequently stressed. These items are at risk for damage accumulation wear out types of failure mechanisms and will require long term durability analysis.

e. Perform thermal stress analysis to:

f. Predict the maximum temperature of an electronic module, and the temperature of its individual components, due to internal heating, when subjected to various power and usage loading conditions.

g. Identify items that are at risk for early failure due to excessive thermal stresses. These items will require long term durability analysis.

9.2.14 Sneak Circuit Analysis (SCA)

Purpose:

To analyze a system to identify and eliminate or control latent conditions that may that may cause occurrence of an unwanted function or the inhibition of a desired function.

Process Description:

a. Perform a structured analysis to uncover the following types of latent or sneak conditions:

b. Sneak paths - Unexpected paths along which current, energy, or logical sequence flows in an unintended direction;

c. Sneak timing - Events occurring in an unexpected or conflicting sequence;

d. Sneak indications - Ambiguous or false displays of system operating conditions that may cause the system or operator to take an undesired action;

e. Sneak labels - Incorrect or imprecise labeling of system functions (e.g., system inputs, controls, displays, and buses) that may cause an operator to apply an incorrect stimulus to the system.

9.2.15 Stress and Damage Simulation Analysis

Purpose

To determine or predict when a specific end-of-life failure mechanism will occur for an individual part in a specific application. The damage simulation approach of predicting the reliability of electronics systems is founded on the fact that fundamental mechanical, electrical, thermal, and chemical processes govern failure mechanisms. The analysis may be used for accepting a design, if the estimated minimum time to failure is greater than the desired design life; performing a sensitivity analysis which reveals the sensitivity of the package lifetime to the package geometry, material properties, operating conditions, and environmental attributes; altering design parameters, according to sensitivity analysis results, to raise the minimum time to failure to the desired design life; or computing the time to failure for potential failure mechanisms. It can also be used to plan tests or screens, and to determine electrical, mechanical, and environmental stress margins.

Process Description

Base highly critical component reliability predictions, when sufficient field data is not available, on a scientific determination of the dominant failure mechanisms and failure sites within the part, by characterizing the stresses in the system using models derived from fundamental principles and experiments widely accepted by the scientific community.

9.3 RMAD Testing Tasks

9.3.1 Reliability Life Testing

Purpose: To validate estimates of a product's lifespan. This requirement is suited to long missions, extended usage, or components of unknown lifespan and reliability.

Process Description: Perform tests under operating conditions which are more severe than those expected during the product's useful life to determine its lifespan in accelerated time. Reliability life testing is conducted under accelerated operating conditions to induce failures at a rate and severity indicating that end-of-life has been reached.

9.3.2 Reliability Development/Growth Testing (RD/GT)

Purpose

To improvement the reliability of an equipment through the systematic and permanent removal of failure mechanisms. Achievement of reliability growth is dependent upon the extent to which testing and other improvement techniques have been used during development and production to "force out" design and fabrication flaws, and on the rigor with which these flaws are analyzed and corrected. The rate at which reliability grows is therefore dependent on how rapidly activities in this iterative loop can be accomplished, how real the identified problems are, and how well the redesign effort solves the identified problems.

Process Description

Establish a reliability growth program that is the result of an iterative design process. The delivered product is field tested to identify actual sources of failures or analyzed to identify potential sources of failures. Further design effort is then spent on correcting these problem areas. The design effort can be applied to either product design or manufacturing process design. There are three essential elements involved in achieving reliability growth:

Detection of failure sources (by analysis and test)

Feedback of problems identified

Effective redesign effort based on problems identified

9.3.3 RMAD Testing Tasks

Purpose

To conduct field testing to determine conformance to specified, quantitative reliability, maintainability, or availability requirements as a basis for qualification or acceptance. This process is implemented to answer the question, “Does the operational system meet or exceed the specified RMAD requirements?”

Process Description

Plan and implement reliability, maintainability, and availability demonstration (RMAD) test procedures, with respective to accept/reject criteria and measurement parameters, to evaluate the operational reliability, maintainability, or availability of the delivered product. The RMAD test plan shall describe how the equipment/system will be tested, the specified test conditions (e.g., environmental conditions), test measurement parameters, length of test, equipment operating conditions, accept/reject criteria, and test reporting requirements.

9.3.4 Design of Experiments

Purpose

To assess one or more independent factors which affect the output of a product or process, and identify the changes needed to achieve the optimum performance of that output. DOE is a useful tool for improving the durability of safety-critical or mission-critical components and assemblies. For this application, the selected product output is a operating life metric (e.g., mean-time-between-failures, mean-mission-duration, mean-time-to-failure, etc.), and the independent factor’s measurements may include censored, suspension, or interval data.

Process Description

Define and implement a DOE process that includes the following steps:

a. Select the product or process output to be optimized

b. Select the independent factors to be assessed

c. Select the measurements to be taken for each independent factor

d. Select the appropriate orthogonal array to record the data

e. Run a set of DOE tests

f. Analyze the test results

g. Calculate the settings needed to optimize the selected output of the product or process

h. Implement design changes in the product or process to incorporate the settings
i. Run confirmation tests to verify that the output is truly optimal

DOE establishes a “Cause-Effect” relationship between the selected product or process output (A.K.A. response) and one or more independent factors influences that output. A set of DOE tests is run at different values (A.K.A. levels) of the independent factors. Each test run involves a unique combination (A.K.A. treatment) of the factor’s levels. When the same number of response measurements is taken for each treatment, the set of DOE tests is labeled a “balanced” experiment. When identical response measurements are recorded for a particular treatment, the identical measurements are labeled “replicate” measurements. The number of treatments taken in a set of DOE tests is determined by the number of factor levels measured in each treatment.

9.3.5 Ongoing Reliability Testing (ORT)

Purpose

To periodically conduct factory testing to determine conformance to specified quantitative reliability requirements as a basis for qualification or acceptance. This process is implemented to answer the question, “Does the development process provide a product that meets or exceeds the specified reliability requirements at time of delivery?”

Process Description

To periodically test samples of the product under nominal conditions that are similar to those expected during the product’s useful life, to ensure the product is reliable at time of delivery.

10. QUALITY ASSURANCE (QA) PROGRAM

The contractor shall assign a quality assurance manager to implement the quality assurance requirements of the program commensurate with the contractual requirements. .

10.1 Quality Assurance Management Processes

10.1.1 Quality Assurance Program Planning

Purpose: To identify the activities required to assure all product qualification requirements are met during design, manufacturing, and assembly.

Process Description: Prepare a QA Program Plan to minimize specification discrepancies.

10.1.2 Subcontractor & Supplier Quality Assurance Management

Purpose: To identify sources of products and services that may be used to satisfy QA requirements, and to manage the pertinent activities of subcontractors and suppliers to minimize risk of specification discrepancies. Assure QA activities of the subcontractor or supplier are consistent with the overall QA Program, by being provided with verification of compliance, or being allowed to conduct surveillance of their reliability activities.

Process Description: Exercise monitoring and control of subcontractor and supplier QA activities; assure that their QA program plans are complete and executable; exchange applicable QA lessons; and assist in development of their QA capabilities. All QA deliverables expected from the subcontractor shall be called out in contractual agreements with the subcontractor.

10.1.3 QA Working Group

Purpose: To conduct formal and informal technical reviews, as necessary, determine the status of the QA program, and work specification discrepancy risks and issues to closure.

Process Description: QA engineers meet and review status of planned QA activities, significant specification discrepancy risks, and any verified out-of–spec conditions. The group also assures required follow-up actions or corrective actions are taken in a timely manner, and are properly implemented, verified, and documented.

10.1.4 Failure Reporting, Analysis and Corrective Action System (FRACAS)

Purpose: To establish and implement a closed-loop system for recording and analyzing anomalies, determining the appropriate correction action, tracking actions to closure, and reporting on anomaly occurrence status. Assures failures which occur throughout the program life cycle receive proper management attention and are resolved in a timely manner.

Process Description: Establish a FRACAS process and database, report, verify, analyze, and correct hardware and software anomalies, monitor closure status of anomalies; and provide FRACAS data to other engineering functions (e.g., statistical failure analysis).

10.1.5 Failure Review Board (FRB)

Purpose: To review failure reports and trends, recommend or assess corrective actions, and assure that the approved corrective actions are implemented in a timely manner.

Process Description: Establish and charter a formal board that is empowered to review failure reports and trends, recommend or assess corrective actions, and assure that the approved corrective actions are implemented in a timely manner.

10.1.6 Critical Item Risk Management (CIRM)

Purpose: To assure all high unit-value systems are to identify and control items whose failure can significantly affect system safety, availability, design life, mission success, or total maintenance/logistics support cost.

Process Description: Establish and maintain an effective method for identification, control and test of critical items from initial design through final acceptance of the system. The method(s) the used for critical item control are clearly described to ensure that all affected personnel such as design, purchasing, manufacturing, inspection, and test are aware of the essential and critical nature of such items. Periodic reviews are planned and executed to determine if additions or deletions to the critical item list and control plan(s) and procedures are warranted, and to assess the effectiveness of the critical item controls and tests. Each critical item control method and plan to be used is subject to on-going review and evaluation.

10.1.7 Project Mission Assurance Database System

Purpose: To establish and maintain a database that contains engineering data which:

a. Identifies the pertinent mission assurance issues and risks, corrective actions, and status of status of closure;

b. Are under data change control and tracking procedures[7];

c. Allows cross-referencing mission assurance analysis models against approved system specifications and design drawings; and,

d. Allows automatic generation of mission assurance reports.

Process Description: The project database will:

a. Identify the pertinent mission assurance issues and risks, corrective actions, and status of closure;

b. Is under data change control and tracking procedures;

c. Allows cross-referencing mission assurance analysis models against approved system specifications and design drawings;

d. Allows automatic generation of mission assurance reports;

e. For Capability 3 and above mission assurance programs, allows an authorized person to indicate particular data is a lessons learned candidate; and,

f. For Capability 4 and above mission assurance programs, contains data records prefaced with one or more keyword data element descriptions (DED)

g. For Capability Level 5 mission assurance programs, describe how non-proprietary lessons learned data will be exchanged with other organizations, e.g., the enterprise will enter into data exchange agreements and employ safeguards to protect security-classified, International Traffic in Arms Regulations (ITAR)-restricted, proprietary, or other sensitive data. The received data will be reviewed by an enterprise-level Lessons Learned Board to identify significant findings that should be implemented on a project or enterprise-wide.

10.1.8 Configuration Management

Purpose: To plan and implement the process which manages changes to approved hardware, software, and project documentation.

Process Description: Establish a configuration management process that manages changes over approved hardware, software, and project documentation.

10.2 Quality Assurance Engineering Tasks

10.2.1 Component Engineering

Purpose: To select reliable electrical, electronic, and electromechanical (EEE) parts prior to the circuit design, and identify EEE parts that are electrically or thermally over-stressed beyond the limits imposed by the part stress derating criteria during the preliminary circuit design.

Process Description: Subject each part to a worst-case part stress analysis at the anticipated part temperature experienced during product qualification testing. This task will be performed during the preliminary circuit design of all developmental hardware products. Part stress derating analysis identifies potential single point failure mode items early.

[7] The objective here is to ensure that all critical items are documented, the history of designed-in safety or reliability improvements is maintained, and current data is distinguishable from out-of-date data.

10.2.2 Process Failure Mode, Effects and Criticality Analysis

Purpose

To analyze an operation / process to identify the kinds of errors which are possible in carrying out the documented procedures, the worst case consequences of those errors on the process (and possibility the product), and the probabilities of those consequences occurring. The process FMECA identifies all process weaknesses that pose an unacceptable risk.

Process Description

Perform a systematic analysis of the in place processes used to manufacture, assemble, test, transport, maintain, and operate the system to identify possible weaknesses or risks, and also evaluate the criticality of each weakness / risk. A process FMECA is prepared whenever a process flow block diagram is available, and should be updated throughout the system development cycle.

10.2.3 Fishbone Analysis

Purpose

To apply a graphical, top-down methodology to identify potential sources of deficiencies based on groups of process areas. The deficiencies are documented using compact Cause and Effect diagrams (hence, the name “Fishbone” Analysis) which apply only “OR” logic in associating end effects and possible causal sources. The compensating features are documented on separate disposition forms which relate back to the fishbone diagram through the indentured numbering scheme, providing unique identification numbers for each fishbone diagram element. Fishbone Analysis can be advantageous in real-time capturing of process interactions and assess deficiency information during working group meetings.

Process Description

Apply the Fishbone Analysis process to capture process interactions and assess deficiency information during working group meetings, when the application of only “OR” logic in associating deficiencies and possible causal sources is sufficient.

10.3 Quality Assurance Testing Tasks

10.3.1 Environmental Stress Screening

Purpose: To plan and conduct screening tests on EEE and mechanical parts, components, or assemblies to identify defective items so that they may be segregated from identical items that passed the screening. For space programs, these items are typically piece parts or assemblies.

Process Description: Develop ESS plans that identify the items to be screened during the production phase and the screens to be applied. Define a methodology for:

a. Determining the environmental stresses sufficient to screen out latent defects that would otherwise be observed in the field; and,

b. Assuring that they are detected prior to integration into the next higher level of assembly.

Conduct tests during the production phase to precipitate flaws, detect the failures, and remove the defective screened items. Quantify the latent defects that will remain in the product at delivery and their impact on field reliability.