GEIA-STD-0009

ANSI/GEIA-STD-0009-2008
Approved: November 13, 2008

ITAA STANDARD

Reliability Program Standard for Systems Design, Development, and Manufacturing

GEIA-STD-0009

August 2008

INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

NOTICE

ITAA Engineering Standards and Publications are designed to serve the public interest by eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards and Publications shall not in any respect preclude any member or nonmember of ITAA from manufacturing or selling products not conforming to such Standards and Publications, nor shall the existence of such Standards and Publications preclude their voluntary use by those other than ITAA members, whether the standard is to be used either domestically or internationally.

Standards and Publications are adopted by ITAA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, ITAA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard or Publication.

This ITAA Standard is considered to have International Standardization implications, but the ISO/IEC activity has not progressed to the point where a valid comparison between the ITAA Standard and the ISO/IEC document can be made.

This Standard does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this Standard to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(Formulated under the cognizance of the ITAA G-47, Systems Engineering Committee, Reliability and Maintainability Subcommittee.)

Published by

Standards & Technology Department
1401 Wilson Boulevard, Suite 1100
Arlington, VA 22209

Information Technology Association of America
(ITAA)

Reliability Program Standard for Systems Design, Development, and Manufacturing

GEIA-STD-0009

Revision	Description of change	Date
-	Initial Release	Aug 2008

Table of Contents

List of Figures

List of Tables

Foreword

Since the cancellation in 1998 of MIL-STD-785B, *Reliability Program for Systems and Equipment Development and Production,* the government has not released a replacement government reliability standard for use in contractual documents that describes the kinds of reliability management practices and reliability design and testing activities the customer will want developers to propose. A reliability standard is needed that aligns with best practices, but is not prescriptive in terms of reliability tasks or methods to be performed. Rather, developers are considered equal partners in deciding which reliability methods are applicable. This standard addresses those needs.

This standard is intended to align best practices of reliability management, design and testing with reliability methods that provide the most value and the least risk in terms of achieving reliable products. The demand for highly-reliable systems/products prompted the development of a new standard that specifies a scientific approach to reliability design, assessment, and verification, coupled with integrated management and systems engineering. This standard defines "what to do" in order to design and build reliability in, then maintain high reliability when the system/product is in the hands of the user.

Acknowledgments

This document was developed and written by a team of subject matter experts (SME) from industry, DoD, academia, research institutes, the military services, and other government agencies. The core working group team members are:

Jim Ruma	General Dynamics Corporation
Paul Shedlock	Raytheon
Dmitry Tananko	General Dynamics Corporation
Michael Cushing	Army Evaluation Center
Bruce Douty	Harris Corporation
Bill Wessels	University of Alabama, Huntsville
Ron Kramer	NSWC, Carderock Division
Margie Hockenberry	Army Materiel Systems Analysis Activity
Gordon Tillery	OSD-DOTE
Chris Sautter	University of Alabama, Huntsville
David Nicholls	Reliability Information Analysis Center
Andrew Long	OSD-DOTE
Ernest Seglie	OSD-DOTE
Chris Denham	GEIA

Since the inception of this effort in late 2007, many people and organizations have contributed to the research and writing of this standard. Throughout, the Core Working Group received continued assistance from the following:

1. Dr. Larry H. Crow, Crow Reliability Resources, Inc., Madison, AL
2. Robert W. Deppe, Boeing Seattle, Seattle, WA

Introduction

The main body of this standard consists of the following four objectives:

1. Understand Customer/User Requirements and Constraints
2. Design and Redesign for Reliability
3. Produce Reliable Systems/Products
4. Monitor and Assess User Reliability

It is important to note that this standard is focused on the attainment of Operational Reliability that meets the customer's documented expectation and requirements. Operational Reliability includes hardware and software failures but also includes other common failure causes such as manufacturing, operator error, operator maintenance, training, quality, etc. These other failure causes are often associated with human factors, but may also include a design element associated with the failure causes. These non- hardware/software failure causes often contribute up to 30 % or more to the Operational Reliability failure rate and must be considered early in development for a comprehensive and successful reliability program.

The Working Group reviewed various documents before drafting this standard, especially Military Standard 785, Reliability Program for Systems and Equipment Development and

Production, which was cancelled in July, 1998, and the new industry standards that were issued at that time as alternatives:

- IEEE 1332, Standard Reliability Program for the Development and Production of Electronic Systems and Equipment, 1998
- SAE JA1000, Reliability Program Standard, June, 1998

The two commercial standards are quite similar, consisting primarily of the first three objectives above, but lacking substance with respect to the essential, reliability program activities.

In August, 2005, the US Department of Defense published the DoD Guide for Achieving Reliability, Availability, and Maintainability (hereafter the "RAM Guide"). The RAM Guide was structured using the three objectives from the commercial standards, plus the fourth objective listed above. The RAM Guide provided ample guidance or "how to" with respect to each objective, but did not identify the activities or "what to do" in order to achieve each objective. Only the reliability portion of the RAM Guide was used by the Working Group to
(1) base this standard on the four objectives above,
(2) identify those activities essential to the achievement of these objectives, and
(3) draft implementing language.

A separate implementation guide has not yet been developed for this standard. In the interim, the RAM Guide can be used for this purpose. It focuses on what can be done as part of a robust systems-engineering process in order to achieve satisfactory levels of reliability, successfully demonstrate them during operational test and evaluation, and sustain them throughout the system/product life cycle. Cross references from objectives of this standard to the RAM Guide are as follows:

GEIA-STD-0009 Objective	RAM Guide Chapter
Objective 1: Understand customer/user requirements and constraints	Chapter 3 focuses on development of RAM metrics and pre-acquisition activities
Objective 2: Design and redesign for reliability	Chapter 4 focuses on successful approaches for designing-in reliability through pre-production testing
Objective 3: Produce reliable systems/products	Chapter 5 focuses on the production reliability starting with limited production
Objective 4: Monitor and assess user reliability	Chapter 6 focuses on monitoring and managing reliability once it is in the hands of the user

Although GEIA-STD-0009 was designed for use with the DOD RAM Guide, the Guide is not required to use this standard. A copy of the guide is available on the internet at URL http:/ www.acq.osd.mil/sse/docs/**RAM_Guide**_080305.pdf or by contacting OUSD (AT&L) DS/SE/ED via ATL-ED@OSD.MIL.

Finally, a successful reliability program is greatly dependent on the demonstrated level of commitment by user's, customer's, and developer's program management, particularly at the upper levels. This commitment can be reinforced by ensuring that the reliability program is an integral part of the business strategy with an optimum funding profile for design, development, verification and demonstration, and operation.

1 Scope

This standard requires the developers and customer/user's working as a team to plan and implement a reliability program that provides systems/products that satisfy the user's requirements and expectations. The user's requirements and needs are expressed in the form of the following four reliability objectives:

- **The developer shall solicit, investigate, analyze, understand and agree to the user's requirements and product needs.** The developer, working with the customer and user, shall include the activities necessary to ensure that the user's requirements and product needs are fully understood and defined, so that a comprehensive design specification and Reliability Program Plan can be generated.
- **The developer shall use well-defined reliability- and systems-engineering processes to develop, design, and verify that the system/product meets the user's documented reliability requirements and needs.** The developer shall implement a set of engineering activities (included in this standard as normative activities and informative activities, refer to Section 3) so that the resulting system/product satisfies the customer's documented requirements and needs.
- **The multifunctional team shall verify during production that the developer has met the user's reliability requirements and needs prior to fielding.** The developer shall include activities that assure the customer that the reliability requirements and product needs have been satisfied.
- **The multifunctional team shall monitor and assess the reliability of the system/product in the field.** The team is responsible for identifying the data elements to assess the reliability of the system/product in the field and to ensure the data collected are accurate and complete. The team will establish a closed-loop feedback method to flow recommended improvements (corrective actions) for monitoring reliability growth.

1.1 Approach

This standard defines a systematic approach to engineering or reengineering a system/product, incorporating best practices that have evolved considerably in recent years. The systematic approach of this standard is applicable for:

- Completing corrective actions,
- Making refinements,
- Developing derivatives,
- Producing modifications,
- Updating existing products,
- Creating and realizing new systems,
- Allowing for the safe and cost-effective disposal (retirement) of a system/product.

This approach is incrementally applied in an engineering life cycle framework that can be implemented during any one or more phases of an enterprise-based life cycle (for example, during production, operations, support, or disposal). The defined approach has two premises:

- A system/product is an item that may consist of hardware, software, firmware, facilities, data, materials, personnel, services, techniques, and processes.

- The engineering of a system/product is accomplished by applying a set of processes to each element of its hierarchy by a multifunctional team of people who have the requisite knowledge and skills.

1.2 Reliability Program Plan and Reliability Case

This standard requires customers and developers operating as a multifunctional team to cooperatively define, document and integrate their reliability processes to ensure systems/products are developed and manufactured to be highly reliable and sustainable over their life cycle. The Reliability Program Plan and Reliability Case are integral to this process. At the beginning of a new development or major modification program, the development team in conjunction with the user, should employ a continuous assessment process to define and document the capability and limitations imposed by the level of reliability, maintainability, system health, and availability with an emphasis on the operational impacts. Whereas the Reliability Program Plan takes a forward view by describing the activities together with any applicable success criterion that are to be undertaken to demonstrate that the Reliability requirements objectives have been achieved, the Reliability Case provides a retrospective view. The Reliability Case provides the record (evidence) of how well the requirements have been demonstrated at each program phase and provides the evidence that the developer achieved the reliability requirements.

The evidence is typically a sequence of reports that demonstrate the developer's actions and analyses to achieve the reliability requirements. A well-documented Reliability Case will greatly benefit any acquisition process, but the retrospective view (as compared to the forward view of the Reliability Program Plan) has historically allowed it to be neglected if the acquisition program has been successful at achieving the reliability requirements defined in the Reliability Rationale. If the reliability requirements are not clearly achieved, the benefits of the Reliability Case increase immensely as the Reliability Case documents the steps that were taken to meet Reliability requirements. The Reliability Case evolves from the direction of the customer and the developer as the project matures. Initially the customer is the acquisition organization; eventually, it is the user.

1.3 Tailoring

This standard does not specify the details concerning "how to" engineer a system/product for high reliability. Nor does it mandate the methods or tools a developer would use to implement the process requirements. The tailoring is dependent upon customer's funding profile, developer's internal policies and procedures and negotiations between the customer and developer.

1.4 Organization

The standard is organized as described in Table 1:

Table 1 Organization of Standard

Section	Title	Description
2.0	Informative References	Lists other standards that are referred to in the text.
3.0	Definitions	Gives definitions for words that are used in a specific technical way in the body of the standard. Only those terms for which the normal dictionary definition does not suffice are included.
4.0	Objective 1: Understand Customer/User Requirements and Constraints	The first objective defines the reliability requirements, assessment/success criteria, controls and responsibilities of all organizations involved for program success.
5.0	Objective 2: Design and Redesign for Reliability	The focus of this second objective is on designing a system/product that satisfies reliability specifications, user requirements, and is both producible and sustainable.
6.0	Objective 3: Produce Reliable Systems/Products	The purpose of this objective is to ensure that systems/products are manufactured with minimum impact on the inherent reliability during the execution of Objective 2.
7.0	Objective 4: Monitor and Assess User Reliability	The purpose of this objective is to establish and execute the requirements of a field reliability monitoring system comprised of data collection, analysis, maintenance and closed-loop feedback activities
Annex A	Methods Matrix	Methods and tools that support the normative activities in Objectives 1 - 4
Annex B	Reliability Best Practices	Describes the recommended reliability program best practices that may be used to ensure that the reliability program requirements are met during the execution of Objectives 1 through 4.
Annex C	Key Documents Matrix	Provides references for the detailed "how to" for the various reliability activities for each objective.
Annex D	Known Failure Definition and Scoring Criteria	References to mandatory failure definition and scoring criteria of the DoD Services.
Annex E	Acronyms	List of acronyms used in this standard

1.4.1 Structure of Objectives

Each of the four reliability objectives described herein is structured as follows:

- Introduction
- Mission and Goals
- People and Organizations

- Supporting Information (Normative)
  - Input Information (Normative)
  - Developed Information (Normative)
- Activities, Methods, and Tools
  - Activities (Normative)
  - Methods and Tools (Informative)
- Output and Documentation (Normative)

The *Introduction* briefly introduces the objective. The subsection, *Mission and Goals*, provides additional background and context that are needed so one can develop a clear understanding of this objective. It is followed by a *People and Organizations* subsection which introduces considerations of personnel and organization that must be addressed when designing reliability into a product. The *Supporting Information* subsection contains two parts. The first part, *Input Information*, lists essential input information that is needed in order to accomplish this design-for-reliability objective. The second part, *Developed Information*, lists the information that is developed during the accomplishment of this objective. As shown in Figures 1 thru 5, the input information feeds the processes and methods contained in *Activities, Methods, and Tools*. Application of these processes and methods should result in a reliable product. *Activities, Methods, and Tools* contains two parts, a normative (mandatory) set of activities and an informative set of methods and tools that are provided for guidance information only. The developed information that is ultimately provided to other objectives in this standard is listed under *Outputs and Documentation*.

1.4.2 Development and Flow of Information Between Objectives

Figure 1 depicts the information that flows into and out of each objective; the inputs to each objective are often the outputs of another objective.

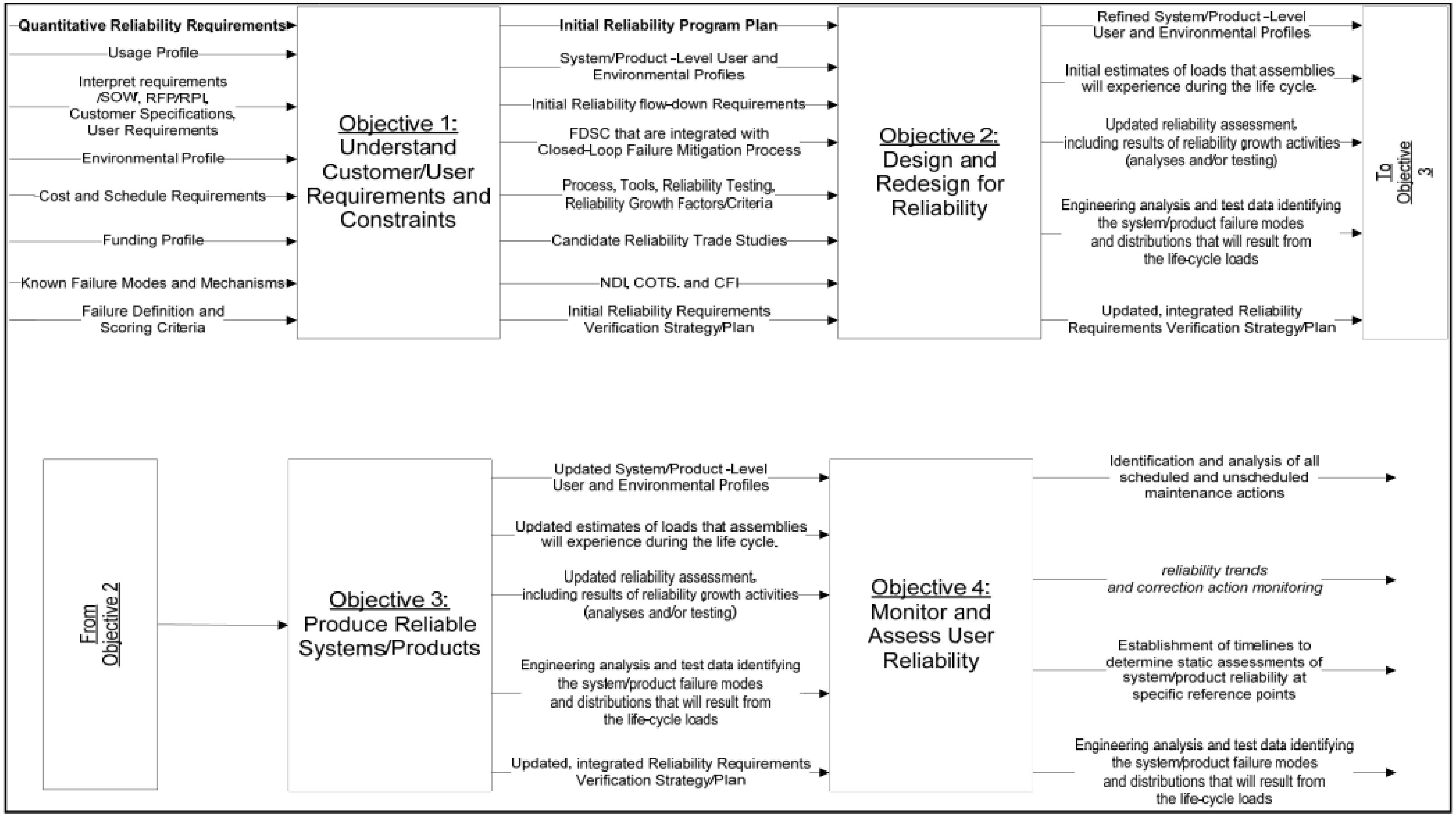

Figure 1 — Information Flow Between Objectives

2 Informative References

The following references were used as guidance for the development of this standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

Crow, Larry H., *Operational Reliability Management,* CRR 522, Crow Reliability Resources, Inc., May 2008

DOD Guide for Achieving Reliability, Availability, and Maintainability, August 3, 2005

GEIA 632 (An American National Standard), *Processes for Engineering a System*

IEEE 1332-1998 (An American National Standard), *Standard Reliability Program for the Development and Production of Electronic Systems and Equipment*, 2 October 1998

MIL-STD-785B Military Standard, *Reliability Program for Systems and Equipment and Development and Production*, 15 September 1980

Reliability Information Analysis Center (RIAC) *Blueprints for Product Reliability*, 15 May 1996

SAE JA1000 1998-06 (An American National Standard), *Reliability Program Standard*

SAE JA1000-1 1999-03 (An American National Standard), *Reliability Program Standard Implementation Guide*

Tiku, Sanjay, *Reliability Capability Evaluation for Electronics Manufacturers*, Ph.D. dissertation, University of Maryland, 2005

3 Definitions

For the purposes of the standard, the following definitions apply.

Term	Definition
Customer	An individual, organization, or enterprise that commissions the engineering of a product, is a prospective purchaser of the product, or is the acquirer of the product.
Capability Maturity Model Integration	Capability Maturity Model Integration (CMMI) provides guidance for defining and improving an organization's processes and the organization's ability to manage the development, acquisition, and maintenance of products and services. CMM Integration places proven practices into a structure that helps the organization assess its organizational maturity and process area capability, establish priorities for improvement, and guides the implementation of these improvements.
Design Reliability	The set of design, development, and manufacturing tasks by which reliability is achieved.
Developer	An enterprise or organization that performs the process requirements of this standard.
Engineering	The engineering of a system/product is accomplished by applying a set of processes to each element of the hierarchy by a multifunctional team of people who have the requisite knowledge and skills.
Environmental Loads	Defined stressing conditions as the result of exposure to natural environments during system/product use. Some typical natural environment stressing conditions are storage and operating temperatures, humidity, diurnal cycles, and solar loading .
Failure	The events, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified under stated conditions for a stated period of time.
Failure Mechanism	The physical, chemical, electrical, thermal, or other process that results in failure. For example: fatigue, fracture, electro-migration, electrical overstress, depletion of material due to mechanical, chemical, electrical, thermal, or other stress.
Failure Mode	The consequence of the mechanism through which an item fails (e.g., short, open, fracture, excessive wear, etc.).
Induced Failure	A failure due to a condition and not due to its own internal failure pattern (e.g., operating outside of specified requirements, environments, or operational procedures, improper handling, support equipment, or operator error).

Term	Definition
Informative Material/Activities	Explanatory material to help the user understand the standard (the informative parts). The informative material is annotated and is contained in notes and informative appendices.
Inherent Failure	A failure that occurs without being caused by the failure of another item.
Inherent Reliability	A measure of reliability which is related to an item's design and its application and is not caused by the failure of another item when the system/product is operated in the specified operation and support environments for a specified duration.
Life Cycle Loads	Stressing conditions as the result of exposure to normal system/product use. Some typical system/product stressing conditions are packaging, handling, shipping and transportation, power on/off cycles, mechanical shock, vibration and maintenance activities (scheduled, unscheduled, recalls, retrofits and software upgrades).
Logistics Footprint	The user's/customer's burden (inventory/equipment, personnel, facilities, transportation assets, supply, and real estate) to deploy, move, and sustain a system/product for a given service use profile.
Multifunctional	A group of individuals representing various product disciplines such as engineering, manufacturing, software, quality, reliability, etc.
Non-operational Reliability	A measure of reliability that is related to an items non-operating design and its application when the system/product is stored in an environmentally protected and/or unprotected location.
Normative Material/Activities	The portion of the standard that prescribes mandatory implementation (the standard itself). Conformance to the standard is judged solely on the basis of the normative material in this standard
Operational Reliability	A measure of the system's/product's performance during the item's operational life that includes the combined effect of the item's design, installation, quality, environment, operation, maintenance, and repair.
Quality Function Deployment	Quality Function Deployment is designed to help planners focus on characteristics of a new or existing product or service from the viewpoints of market segments, company, or technology-development needs. This technique yields graphs and matrices.
Reliability	Reliability is the ability/probability of failure free performance of the system/product, over the expected service use profile and environmental conditions over a given period of time. Reliability is expressed in terms of operational reliability and non-operating reliability.

Term	Definition
Reliability Activity	The set of design, development, manufacturing, and maintenance tasks performed to identify, quantify, and qualify product characteristics in terms of attributes, tolerances, and the test and inspection requirements necessary to produce a reliable, available, and maintainable product.
Reliability Assessment	An activity that quantitatively evaluates reliability using a model, failure definitions and scoring criteria, and the applied life cycle loads and environmental loads
Reliability Case	A reasoned, auditable argument created to support the contention that a defined system/product satisfies the reliability requirements. The Reliability Case report documents the reliability evidence and arguments from the Reliability Case to support the program phases.
Reliability Model	A methodology for estimating the system's/product's ability to meet the specified reliability requirements.
Reliability Verification	Formally determining whether the customers quantitative reliability requirements have been met.
Shall	A mandatory requirement to be followed in order to conform to this standard.
Should	Indicates that there are several possibilities: one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is discouraged but not prohibited.
Supplier	Provides a product or group of products to a customer. The supplier can be a vendor that has a product that does not need development, or a developer that must develop the product or products.
System/Product	A system/product is an end item that may consist of hardware, software, firmware, facilities, data, materials, personnel, services, techniques, and processes.
Systems Engineering	A branch of engineering whose responsibility is creating and executing an interdisciplinary process to ensure that customer and user's needs are satisfied in a high quality, trustworthy, cost efficient, and schedule compliant manner throughout a system's entire life cycle, from development to operation to disposal.
Technical Review	An event at which the progress of the technical effort is assessed relative to its governing plans and technical requirements.
User	Individual, organization, or enterprise that uses, applies, or operates the product.

Term	Definition
Verification	Confirmation by examination and provision of objective evidence that the specified requirements to which the end product is built, coded, or assembled have been fulfilled.

4 Objective 1: Understand Customer/User Requirements and Constraints

4.1 Introduction (Informative)

The focus of the first objective is to develop an understanding of the customer's system/product reliability requirements and constraints (both internal and external) and clearly communicate the developer's understanding of the customer's requirements. The first objective defines the reliability requirements, assessment criteria, controls, and responsibilities of all organizations involved in order to ensure program success. Figure 2 graphically depicts the operation of this Objective.

Reliability is the ability/probability of the system/product to perform its intended functions over the expected user and environmental profile for a given period of time. The failure definitions must be coordinated with the customer because not all failures (hardware, software, firmware, process, procedure, or user) are reliability failures but must be assessed for potential corrective action. Reliability requirements are quantifiable and measurable metrics used to assess the compliance of the contractual requirements.

4.2 Mission and Goals (Informative)

The mission of this objective is to assemble a multifunctional team (user, customer, and developer) to

1. understand the customer's requirements, failure definitions, user and environmental profiles, and
2. influence the design based on the user's needs and constraints.

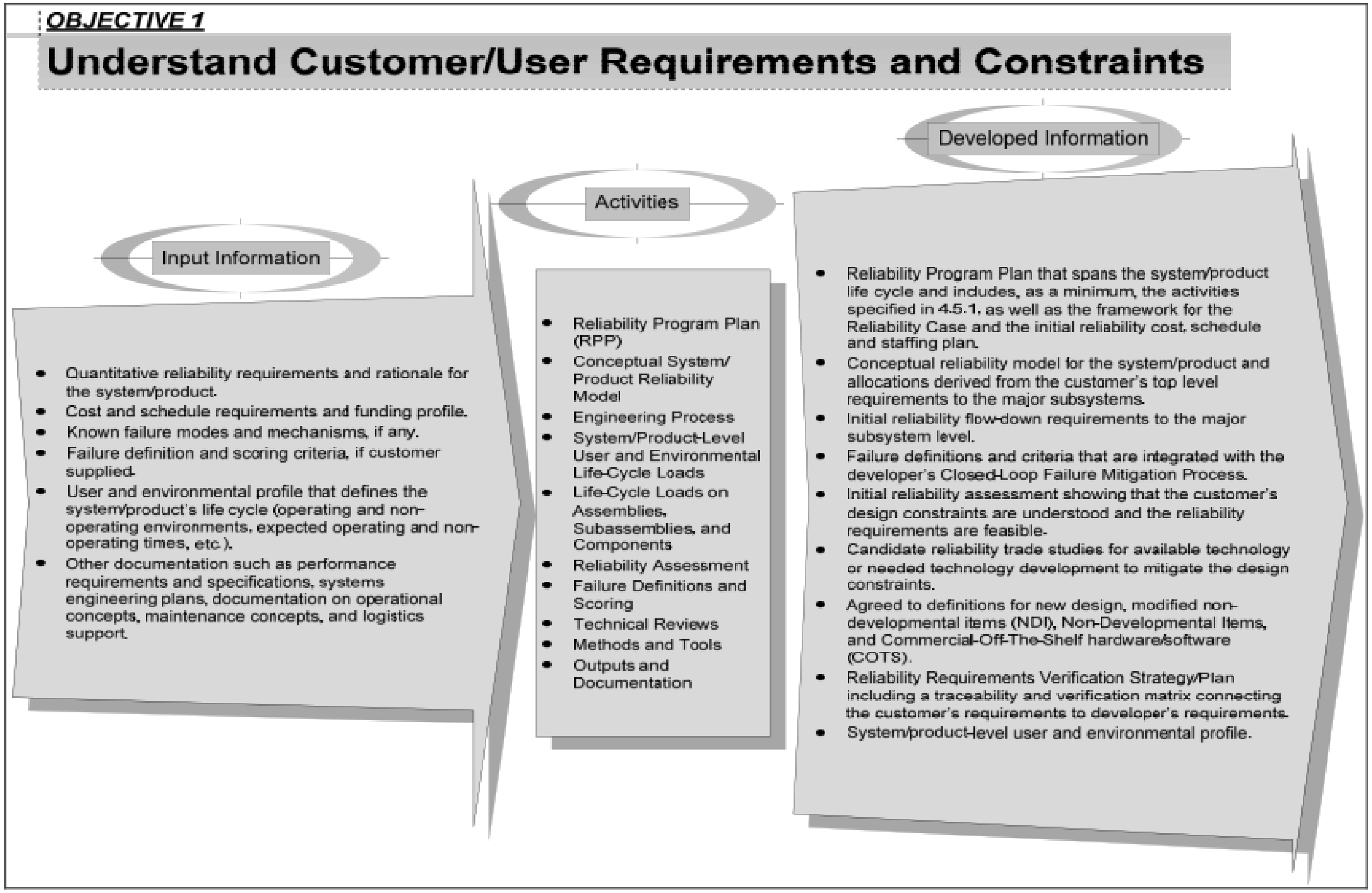

Figure 2 — Objective 1 Inputs, Activities, and Output

4.3 People and Organizations (Normative)

Multifunctional groups shall collaborate during each phase of the program, perceive and mutually understand specific goals and objectives, and define and develop the system/product reliability requirements using a number of industry tools such as Quality Function Deployment (QFD). Customer-User Communication: The customer community must collaborate with the users to define the desired capabilities for a system/product. This capability definition includes design reliability and operational reliability in the smallest logistics footprint. The logistics footprint is a function of system/product's embedded diagnostics and the customer's system/product support plan (spares, maintenance, training, and technical manuals).

Customer-Developer Communication: The customer must communicate the user's desired reliability and performance requirements for the system/product to the developer. The developer's engineering organizations must analyze the requirements and establish a dialogue with the customer so that the developer can complete a detailed requirements analysis to ensure that the requirements are understood and feasible. The developer **shall** communicate the acceptance of the requirements or recommend an alternative to the customer. This communication is necessary to ensure eventual system/product suitability. These communications between the developer and customer should be documented.

User/Customer-Developer Communication: The system/product reliability feasibility assessment (i.e., the assessment of the feasibility of achieving the user/customer requirements) **shall** be completed to the same level as the customer's specification to the developer.

System/product engineering and reliability engineering functions **shall** be responsible for implementing and executing the design-for-reliability methodology over the system/product's life cycle.

The customer will ensure that sufficient funding is available for the developer to provide a system/product that meets requirements when operated and maintained by the user over the system/product's life cycle. The goal is to apply the optimum funding profile for design, development, verification, and deployment at the appropriate time.

4.4 Supporting Information (Normative)

The information listed under Input Information is required in order to enable the developer to design, produce, and deliver a system/product that meets requirements and is suitable to the end user. This information may be provided by the customer or may be jointly developed by the customer/user and developer.

4.4.1 Input Information (Normative)

The following information is required before a reliable system/product can be designed:

- Quantitative reliability requirements and rationale for the system/product.
- Cost and schedule requirements and funding profile.
- Known failure modes and mechanisms, if any.
- Failure Definition and Scoring Criteria, if customer supplied.

- User and environmental profile that defines the system/product's life cycle (operating and non-operating environments (including storage), expected operating and non-operating times, etc.). **For example, miles traveled, percent terrain type, hours of operation, rounds fired, etc.**
- Other documentation such as performance requirements and specifications, system/product engineering plans, system/product test plans, documentation on operational concepts, maintenance concepts, and logistics support.

Rationale for the reliability requirements should include, as applicable,
1. requirements for availability, maintainability, testability, durability, and system health fined as embedded diagnostics, Built-In Test (BIT), and prognostics),
2. customer/user design constraints (e.g., technology, manpower, training, and logistics port),
3. desired maintenance concepts,
4. reliability estimates, support concept, and limitations for similar systems/products, and
5. data on how the system/product will be packaged, handled, shipped, and transported.

4.4.2 Developed Information (Normative)

During the course of designing reliability into a system/product, a considerable amount of information will be developed. In many cases, input information to this objective will be expanded on and updated. The activities in Section 4.5.1 will result in the developer generating this information. The information developed **shall** include:
- Reliability Program Plan that spans the system/product life cycle and includes, as a minimum, the activities specified in Section 4.5.1, as well as the framework for the Reliability Case and the initial reliability cost, schedule and staffing plan.
- Conceptual reliability model for the system/product and allocations derived from the customer's top level requirements to the major subsystems.
- Initial reliability flow-down requirements to the major subsystem level.
- Failure definitions and criteria that are integrated with the developer's Closed-Loop Failure-Mode Mitigation Process.
- Initial reliability assessment showing that the customer's design constraints are understood and the reliability requirements are feasible.
- Candidate reliability trade studies for available technology or needed technology development to mitigate development and associated risks.
- Agreed-to definitions for new design, Non-Developmental Items (NDI), modified NDI, Customer-Furnished Items (CFI), and Commercial-Off-The-Shelf (COTS) hardware/software.
- Reliability Requirements Verification Strategy/Plan including a traceability and verification matrix connecting the customer's requirements to developer's requirements.
- System/product-level user and environmental profile.

4.5 Activities, Methods, and Tools

This section is divided into two parts. The first part specifies the normative activities that the developer **shall** perform. The second part is informative in nature and lists methods and tools that the developer may consider to effectively support the normative activities.

All activities, methods and tools used should be evaluated and applied in a manner that adds demonstrated value to the program, at an optimized life cycle cost and utilization of resources, in support of the stated mission and goals of this Objective.

4.5.1 Activities (Normative)

4.5.1.1 Reliability Program Plan (RPP)

The developer **shall** develop a program for designing, manufacturing, and sustaining reliable systems/products. The RPP **shall** be tailored to each system/product. A RPP should ideally be developed both by the developer (delineating those activities required to meet customer reliability requirements) and the customer (who provides an expansion of the required activities to include the tasks and customer-supplied resources to support and confirm the attainment of reliability requirements). The developer may identify and include additional activities not identified herein. The RPP is initially prepared early in the program and is periodically updated and coordinated with the customer.

The RPP **shall**:

- Plan for the attainment of customer reliability requirements.
- Provide visibility into the management and organizational structure of those responsible and accountable (both developer and customer) for the conduct of reliability activities over the entire life cycle.
- Define all resources (e.g., personnel, funding, tools, and facilities) required to fully implement the reliability program.
- Include a coordinated schedule for conducting all reliability activities throughout the system/product life-cycle.
- Include detailed descriptions of all reliability activities, functions, documentation, processes, and strategies required to ensure system/product reliability maturation and management throughout the system/product life cycle.
- Document the procedures for verifying that planned activities are implemented and for both reviewing and comparing their status and outcomes.
- Manage potential reliability risks due, for example, to new technologies or testing approaches.
- Ensure that reliability allocations, monitoring provisions, and inputs that impact reliability (e.g., user and environmental loads) are flowed down to subcontractors and suppliers.
- Include contingency-planning criteria and decision-making for altering plans and intensifying reliability improvement efforts.
- Include, at minimum, the normative activities identified throughout this standard.
- Include, when applicable, additional customer-specified normative activities.

The RPP **shall** address the implementation of all the normative activities identified in Objectives 1 - 4:

- <u>System/Product Reliability Model and Requirements</u>:
  Describe
  1. the methods and tools that will be used to build and refine the system/product reliability model and requirements,
  2. the extent to which detailed component stress and damage models will be incorporated in the system/product reliability model,

3. how the system/product reliability model and requirements will be updated as the system/product design evolves and as failure modes are identified during the analysis of test and field failures, and
4. how the system/product reliability model and requirements will be used to identify reliability-critical items.

- Engineering Process:
  Describe
  1. how it will be ensured that the normative reliability activities are an integral part of the systems-engineering process,
  2. how reliability-improvement actions will routinely be incorporated into the design and manufacture of the system/product,
  3. how it will be ensured that design rules that impact reliability, including parts, materials, process review, selection, and control, parts stress derating, electrical, mechanical, thermal and other guidelines, are adhered to,
  4. how reliability-critical items will be identified, managed, and controlled, and
  5. how the reliability impact of system/product design changes and supplier change notices will be monitored and evaluated.

- System/Product-Level User and Environmental Life-Cycle Loads:
  Describe
  1. how and when the developer will develop, refine, and verify the estimates of system/product-level user and environmental life-cycle loads, and
  2. requirements, if any, for access to customer assets.

- Life-Cycle Loads on Subsystems, Assemblies, Subassemblies, and Components:
  Describe
  1. how and when the developer will prepare and refine estimates of the life-cycle loads that subordinate assemblies, subassemblies, components, COTS, NDI, and CFI will experience as a result of system/product-level user and environmental loads,
  2. how and when teams (a) developing assemblies, subassemblies, and components and (b) selecting and integrating items not specifically developed for this system/product, will receive these estimates and updates.

- Identification of Failure Modes and Mechanisms:
  Describe
  1. how and when failure mechanisms and modes that may result when the estimated life-cycle loads are imposed on the system/product will be identified for items specifically developed for this system/product as well as for items being selected and integrated into it, and
  2. how the developer will ensure that test and field failures are analyzed to root cause.

- Closed-Loop Failure-Mode Mitigation Process:
  Describe
  1. strategies for monitoring, assessing, prioritizing, and communicating the status of test and field failures throughout the organization,
  2. strategies for identifying, developing, and approving design and/or process corrective actions to eliminate root failure causes throughout the system/product life cycle,

3. how the implementation of corrective actions will be verified and their effectiveness tracked,
4. how lessons learned will be documented, reviewed, and communicated, and
5. how root-cause analysis of test and field failures will be used to improve the reliability of the system/product.

- Reliability Assessment:
  Describe
  1. how and when reliability assessments will be performed (including, when applicable, customer-specified reliability values that must be achieved at various points during development) and documented in the Reliability Case,
  2. which assessment methods will be used, and
  3. how design and process changes are documented, monitored, and evaluated for their impact on reliability.

- Plan Design, Production, and Field Reliability Verification:
  Describe
  1. the strategy for verifying the satisfaction of customer reliability requirements,
  2. the activities to be performed and processes to be used that will ensure that inherent reliability levels are not degraded during subsequent phases of the system/product life cycle.

- Failure Definitions and Scoring:
  Describe how the failure definitions and scoring criteria will be used during development to minimize the occurrence of failures in the field when actual users operate and maintain the system/product.

- Technical Reviews:
  Describe how and when technical interchanges and reviews will be conducted.

- Methods and Tools:
  Describe
  1. the methods and tools that will be used to implement the normative reliability activities, and
  2. the design-reliability best practices to be used and how adherence to them will be ensured.

- Outputs and Documentation:
  Describe how and when the outputs that will be generated during the execution of the normative activities will be documented and distributed.

4.5.1.2 Conceptual System/Product Reliability Model

The developer **shall** understand the rationale for the customer's reliability requirements and conduct scheduled technical interchanges with the customer in order to facilitate this understanding. The developer **shall** develop a conceptual reliability model for the system/product. The conceptual reliability model

1. relates subsystem-level reliability to system/product-level reliability, and
2. presents a clear picture of functional interdependencies, redundancies, and degraded modes of operation, and provides the framework for developing quantitative, system/product-level reliability estimates to guide the design trade-offs process.

4.5.1.3 Engineering Process

Systems engineering is an iterative process of top-down synthesis, development, and operation of a system/product that satisfies the full range of requirements for the system. The systems-engineering process translates customer/user needs and requirements into suitable systems/products while balancing performance, risk, cost, and schedule.

The developer **shall**

1. incorporate the reliability activities as an integral part of a disciplined and documented systems and/or design engineering process and plan,
2. submit the potential reliability improvements identified during the execution of the reliability activities to the appropriate engineering organizations,
3. monitor and evaluate the reliability impact of changes to the design or manufacture of the system/product,
4. identify, manage, and control reliability-critical items, and
5. ensure adherence to design rules that impact reliability, including stress derating, electrical, mechanical, thermal, and other guidelines.

4.5.1.4 System/Product-Level User and Environmental Life-Cycle Loads

Designing for reliability requires a careful and complete user profile, which includes wartime and peacetime usage rates (if applicable), the use environments, non-operating (including storage) duration and conditions, and the user constraints due to the maintenance and supply systems. The total life-cycle environment can include storage, shipping, handling, installation, and maintenance. The developer **shall** estimate the user and environmental loads (e.g., mechanical shock, vibration, and temperature/humidity cycles due to ambient air temperature and solar loading) that the system/product is expected to encounter in actual usage throughout the life cycle. The estimates of life-cycle loads **shall** be updated periodically and eventually verified with measurements or suitable substantiating data sources approved by the customer. If the information received from the customer regarding the actual user and environmental loads is insufficiently detailed, the developer **shall** seek access to customer assets (e.g., test courses or vehicles that the system/product will be integrated with). The customer **shall** provide this access when requested.

4.5.1.5 Life-Cycle Loads on Assemblies, Subassemblies, and Components

The developer **shall** prepare initial estimates of the life-cycle loads that subordinate assemblies, subassemblies, components, COTS, NDI and CFI will experience as a result of the system/product-level user and environmental loads estimated in Section 4.5.1.4. These estimates **shall** be provided to teams developing assemblies, subassemblies, and components for this system/product. These estimates **shall** also be provided to teams selecting and integrating items not specifically developed for this system/product, which may include COTS, NDI, and CFI, as well as assemblies, subassemblies, and components. The estimates of life-cycle loads **shall** be updated when the system/product-level loads are updated or as the design evolves. The teams that received initial estimates **shall** be provided with these updated estimates.

4.5.1.6 Reliability Assessment

The developer **shall** use the conceptual system/product reliability model developed in Section 4.5.1.2, in conjunction with expert judgment, in order to assess if the design (including COTS, NDI, and CFI) is capable of meeting reliability requirements in the user environment. If the assessment is that the customer's requirements are infeasible, the developer **shall** communicate this to the customer. The developer **shall** allocate the reliability requirements and flow them and needed inputs down to its subcontractors/suppliers.

4.5.1.7 Plan Reliability Verification

The developer **shall** plan activities to ensure that the reliability requirements are met. The developer **shall** develop the Reliability Requirements Verification Strategy/Plan. For complex systems/products, this strategy **shall** include reliability values to be achieved at various points during development. The verification **shall** be based on analysis, modeling & simulation, testing, or a mixture. The user and environmental life-cycle loads developed under the System/Product-Level User and Environmental Life-Cycle Loads activity **shall** be used. Testing **shall** be operationally realistic.

Reliability verification **shall** be an integral part of the overall system/product engineering verification and be coordinated and integrated across all phases. The customer may have specific test requirements (e.g., reliability qualification testing, testing in customer facilities, customer-controlled, customer-scored testing). The customer may choose to review and approve the verification strategy/plan.

4.5.1.8 Failure Definitions and Scoring

The developer **shall** understand the failure definitions and scoring criteria established for the system/product and **shall** develop the system/product to meet reliability requirements when these failure definitions are used and the system/product is operated and maintained by the user. The developer **shall** identify and mitigate human errors,(excluding those due to deliberate maliciousness and/or obviously reckless use) that may occur when actual users operate and maintain the system/product. Particular customers, such as the US Department of Defense (Annex D), may have specialized procedures for defining and scoring failures. In the absence of customer-established failure definitions and scoring criteria, the customer and developer **shall** jointly develop and agree to these.

4.5.1.9 Technical Reviews

The developer **shall** conduct technical interchanges with the customer/user in order to review the status of the Reliability Activities and compare their outcomes. The developer **shall** conduct formal reviews for reliability that promote an understanding of the user environment in which the system/product will operate and to assure progress toward achieving the reliability requirements. The number and formality of these reviews should be tailored to match the complexity of the system/product, the maturity of the technology, and the competitive nature of the industry. Unless the customer specifies requirements for technical interchanges and reviews, the developer will propose a review schedule. As a minimum, these reviews should be considered before each "major" program milestone or gate. Reliability reviews should begin early in the system/product development process and continue through production and deployment. Some of the milestones that should be considered as potential review points are at the completion of:

- customer requirements assessment,
- conceptual design reviews.

4.5.1.10 Methods and Tools

The developer **shall** implement the activities in Section 4.5.1 with appropriate reliability design and development methods and tools. Section 4.5.2 provides an overview of many such methods. The developer **shall** select appropriate methods and describe them in the updated Reliability Program Plan. The customer may elect to review, comment and negotiate regarding the methods selected by the developer. The developer **shall** identify and employ a set of design- and process-reliability best practices.

4.5.1.11 Outputs and Documentation

While executing the activities in Section 4.5.1, a number of outputs will be generated. In many cases, these outputs are inputs that are required by the other objectives in this standard. The developer **shall** document these outputs in an updated Reliability Case or equivalent documentation.

4.5.2 Methods and Tools (Informative)

In order to implement the activities in Section 4.5.1, a variety of reliability methods and tools will be needed. Some of the most popular methods and tools are listed in Annex A. A list of reliability best practices is provided in Annex B.

5 Objective 2: Design and Redesign for Reliability

5.1 Introduction (Informative)

The focus of the first objective in this standard is on understanding and communicating user needs and constraints. The focus of this, the second, objective is on designing a system/product that satisfies reliability specifications and user requirements, and is both producible and sustainable. Figure 3 graphically depicts the operation of this Objective.

5.2 Mission and Goals (Informative)

The mission of this objective is to develop the system/product design so that it meets all design specifications, is producible, and will, when produced and fielded, meet user requirements and needs throughout the life cycle.

Design and development are system/product-engineering processes. Design synthesis that achieves high reliability involves an iteration of design (i.e., design and redesign) where failure modes that would be encountered in the field are systematically identified and removed. The removal or mitigation of failure modes requires vigilant, informed, and sustained engineering effort. Reliability requirements are more likely to be achieved when designers accurately anticipate and accommodate user, environmental, and support conditions that will be encountered in the field.

The developer will use well-defined reliability engineering processes to develop, design, manufacture, and sustain the system/product so that it meets the user's reliability requirements and needs. By starting the reliability design tasks as early as possible in the system/product development, and iterating the design only as necessary, the design will be robust and will therefore minimize impact on cost and schedule.

5.3 People and Organizations (Normative)

The performance of the reliability activities in Section 5.5.1 **shall** be an integral part of the system/product engineering process. The developer **shall** ensure the system/product is designed to meet its reliability requirements by utilizing a multifunctional team of designers that should also include user, manufacturing, finance, test, and support/logistics staff. And, as a minimum, both a developer and customer reliability engineer **shall** be assigned to the multifunctional design team. The developer **shall** document the management structure, roles, responsibilities, and accountability of those responsible for the performance of the system/product and reliability engineering in the Reliability Program Plan.

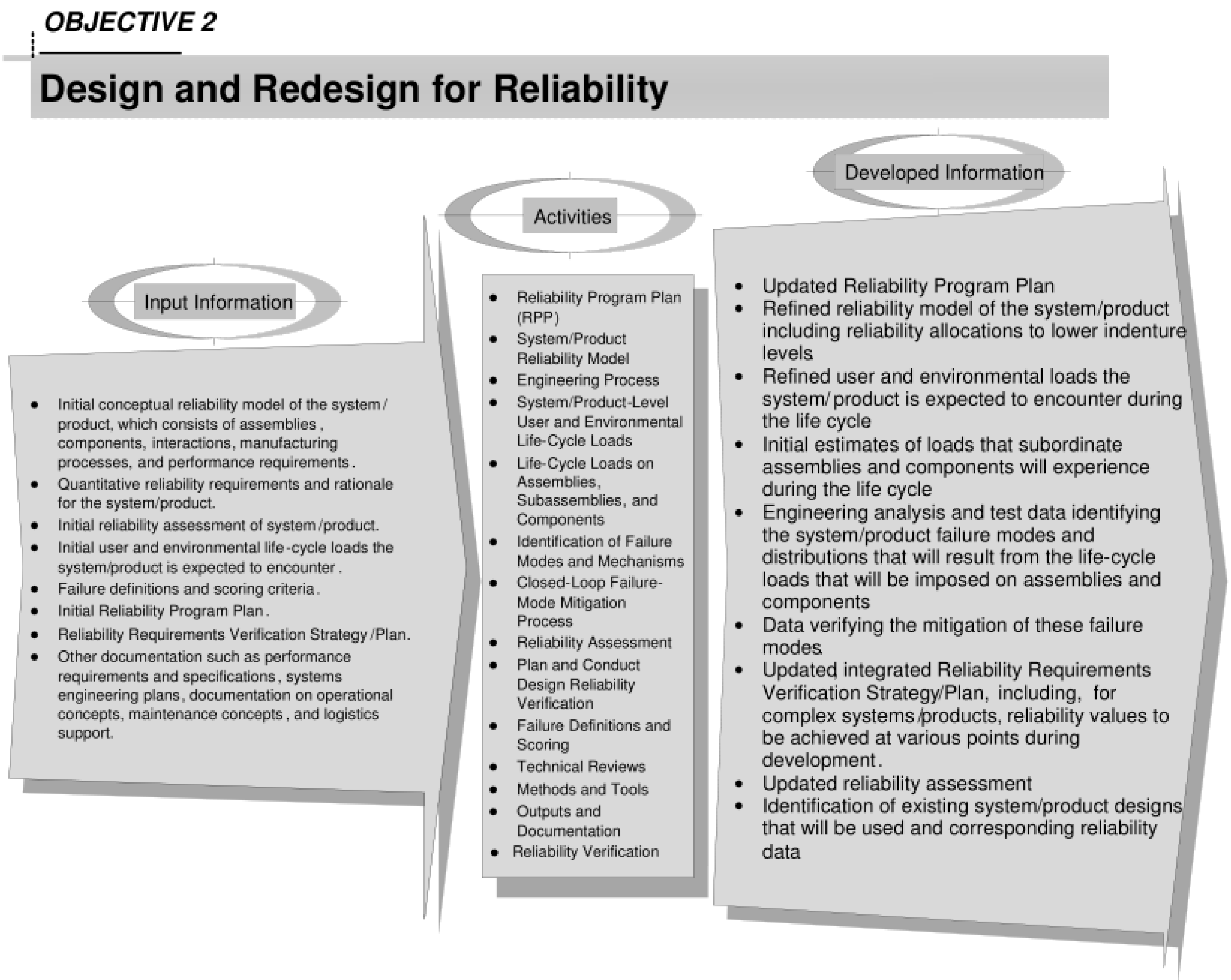

Figure 3 — Objective 2 Inputs, Activities, and Outputs

5.4 Supporting Information

As a minimum, the input information listed under Input Information below is needed in order to begin to design for reliability. Developed Information lists the information that will be developed as reliability is designed into the system/product using the activities in Section 5.5.1.

5.4.1 Input Information (Normative)

The following information is required before a reliable system/product can be designed:

- Initial conceptual reliability model of the system/product, which consists of assemblies, components, interactions, manufacturing processes, and performance requirements.
- Quantitative reliability requirements and rationale for the system/product.
- Initial reliability assessment of system/product.
- Initial user and environmental life-cycle loads that the system/product is expected to encounter.
- Failure definitions and scoring criteria.
- Initial Reliability Program Plan.
- Reliability Requirements Verification Strategy/Plan.
- Other documentation, such as performance requirements and specifications, system/product engineering plans, documentation on operational concepts, maintenance concepts, and logistics support.

Nearly all of the data items listed above are outputs from other objectives of this standard.

5.4.2 Developed Information (Normative)

During the course of designing reliability into a system/product, a considerable amount of information will be developed. In many cases, input information to this objective will be expanded on and updated. The activities described in Section 5.5.1 will result in this developed information. The information developed **shall** include:

- Updated Reliability Program Plan.
- Identification of existing system/product designs that will be used and corresponding reliability data.
- Refined reliability model of the system/product, including reliability allocations to lower indenture levels.
- Refined user and environmental loads that the system/product is expected to encounter during the life cycle.
- Initial estimates of loads that subordinate assemblies and components will experience during the life cycle.
- Engineering analysis and test data identifying the system/product failure modes and distributions that will result from the life-cycle loads that will be imposed on assemblies and components.
- Data verifying the mitigation of these failure modes.
- Updated, integrated Reliability Requirements Verification Strategy/Plan, including, for complex systems/products, reliability values to be achieved at various points during development.
- Updated reliability assessment.

5.5 Activities, Methods, and Tools

This section is divided into two parts. The first part, Section 5.5.1, specifies the normative activities that the developer **shall** perform. The second part, Section 5.5.2, is informative in nature and lists methods and tools that the developer may consider to effectively support the activities in Section 5.5.1.

All activities, methods and tools used should be evaluated and applied in a manner that adds demonstrated value to the program, at an optimized life cycle cost and utilization of resources, in support of the stated mission and goals of this Objective.

5.5.1 Activities (Normative)

5.5.1.1 Reliability Program Plan (RPP)

The developer **shall** follow the current RPP in the performance of all activities in Section 5.5.1. Updates to the RPP **shall** be recommended based on quantified and supporting rationale, with customer involvement and approval.

5.5.1.2 System/Product Reliability Model

The developer **shall** develop a system/product reliability model using the conceptual reliability model developed in Section 4.5.1.2 as a starting point. The system/product reliability model

1. relates component-level reliability to system/product-level reliability, and
2. presents a clear picture of functional interdependencies, redundancies, and degraded modes of operation, and provides the framework for developing quantitative, system/product-level reliability estimates to guide the design trade-offs process.

The developer **shall** build the reliability model by refining the conceptual reliability model developed under the first objective. At minimum, the system/product reliability model **shall** be used to

1. update the reliability allocations from the system/product level down to lower indenture levels,
2. aggregate system/product-level reliability based on reliability estimates from lower indenture levels,
3. identify single points of failure, and
4. identify reliability-critical items.

As failure modes are identified during the analysis of test and field failures, the system/product reliability model **shall** be refined accordingly. Failures that occur either in test or in the field **shall** be analyzed until the root cause failure mechanism is identified. Detailed component stress and damage models **shall** be incorporated as appropriate.

5.5.1.3 Engineering Process

The developer **shall**

1. incorporate the reliability activities as an integral part of a disciplined and documented systems and/or design engineering process and plan,
2. submit the potential reliability improvements identified during the execution of the reliability activities to the appropriate engineering organizations,

3. monitor and evaluate the reliability impact of changes to the design or manufacture of the system/product,
4. identify, manage, and control reliability-critical items, and
5. ensure adherence to design rules that impact reliability, including stress derating, electrical, mechanical, thermal, and other guidelines.

5.5.1.4 System/Product-Level User and Environmental Life-Cycle Loads

The developer **shall** refine the estimates of life-cycle user and environmental loads developed in Section 4.5.1.4. These estimates **shall** be updated periodically and verified with measurements on pre-production systems/products or suitable substantiating data sources approved by the customer.

5.5.1.5 Life-Cycle Loads on Assemblies, Subassemblies, and Components

The developer **shall** estimate the life-cycle loads that subordinate assemblies, subassemblies, components, COTS, NDI, and CFI will experience as a result of the product-level user and environmental loads estimated in Section 5.5.1.4. These estimates **shall** be provided to teams developing assemblies, subassemblies, and components for this system/product. These estimates **shall** also be provided to teams selecting and integrating items not specifically developed for this system/product, which may include COTS, NDI, and CFI, as well as assemblies, subassemblies, and components. These estimates of life-cycle loads **shall** be refined periodically as the system/product-level loads are updated and/or as the design evolves. The teams that receive initial estimates **shall** be provided with these updated estimates. Eventually the estimates **shall** be verified with measurements (e.g., from instrumented pre-production systems/products).

5.5.1.6 Identification of Failure Modes and Mechanisms.

The identification of failure modes and mechanisms **shall** start as soon as the development begins. The estimates of life-cycle loads on assemblies, subassemblies, and components **shall** be used as inputs to engineering- and physics-based models in order to identify potential failure mechanisms and the resulting failure modes. The teams developing assemblies, subassemblies, and components for this system/product **shall** identify and confirm through analysis, test, or accelerated test the failure modes and distributions that will result when life-cycle loads estimated in Section 5.5.1.5 are imposed on these assemblies, subassemblies, and components. The teams selecting and integrating items not specifically developed for this system/product (which may include COTS, NDI, and CFI, as well as assemblies, subassemblies, and components) **shall** identify and confirm, through analysis, test, or accelerated test, the failure modes and distributions that will result when these life-cycle loads are imposed on these items. These failure modes and distributions **shall** be updated as the design evolves and when the life-cycle user and environmental loads are updated. These updates **shall** continue after the system/product is fielded.

Failures that occur in either test or the field **shall** be analyzed until the root cause failure mechanism has been identified. Identification of the failure mechanism provides the insight essential to the identification of reliability improvements. Predicted failure modes/mechanisms **shall** be compared with those from test and the field.

5.5.1.7 Closed-Loop Failure-Mode Mitigation Process

The developer **shall** have an integrated team, including suppliers of assemblies, subassemblies, components, and selectors/integrators of COTS, NDI, and CFI, as applicable, analyze all failure modes and mechanisms arising from modeling, analysis, or test in order to formulate corrective actions.

Failure modes **shall** be addressed and resolved in a timely manner consistent with (1) the criticality of their impact on safety, reliability, and performance requirements and (2) their impact on the total life-cycle cost of the system/product. Failure modes **shall** be mitigated by one or more of the following approaches:

- eliminating the failure modes,
- reducing their occurrence probabilities or frequencies,
- incorporation of redundancy, and/or
- mitigation of failure effects (e.g., fault recovery, degraded modes of operation, providing advance warning of failure).

The developer shall aggressively mitigate failure modes until the reliability requirements can be successfully verified.

The developer **shall** employ a mechanism for monitoring and communicating throughout the organization

1. descriptions of test and field failures,
2. analyses of failure mode and root-cause failure mechanism, and
3. the status of design and/or process corrective actions and risk-mitigation decisions.

This mechanism **shall** be accessible by the customer.

It should be noted that the reliability of any item, including COTS, NDI, or CFI, depends greatly upon the user and environmental loads that are imposed on it. It may be possible to markedly reduce the occurrence probabilities and frequencies of COTS/NDI/CFI failure modes by careful management of these loads by, for example, reducing the loads through the use of thermal or dynamic isolation techniques, or directly modifying the COTS/NDI/CFI so it is more robust (with the understanding of the potential risk of voiding the warranty provisions of the COTS/NDI/CFI supplier).

It may be possible to address some failure modes with multiple approaches (e.g., modifying the design to make it more failure resistant in the hands of users versus attempting to modify the behavior of users). If this is the case, the developer **shall** analyze the alternatives with respect to their impact on failure-mode frequency, maintenance burden, program delay, and life-cycle cost.

All failure modes that are expected to occur during the system/product life cycle **shall** be included in the system/product reliability model.

5.5.1.8 Reliability Assessment

As provided in the Reliability Program Plan, the developer **shall** assess the reliability of the system/product periodically throughout the life cycle. Reliability estimates from analysis, modeling & simulation, and test **shall** be tracked as a function of time and compared against customer reliability requirements. The implementation of corrective actions **shall** be verified and their effectiveness tracked. Formal reliability growth methodology **shall** be used where applicable (e.g., when failure modes are discovered and addressed with a test-analyze-and-fix process) in order to plan, track, and project reliability improvement.

5.5.1.9 Plan and Conduct Design Reliability Verification

The developer **shall** plan and conduct activities to ensure that the design reliability requirements are met. The developer **shall** refine the Reliability Requirements Verification Strategy/Plan initiated under Objective 1. For complex systems/products, this strategy **shall** include reliability values to be achieved at various points during development. The verification **shall** be based on analysis, modeling & simulation, testing, or a mixture. The user and environmental life-cycle loads developed under the System/Product-Level User and Environmental Life-Cycle Loads activity **shall** be used. Testing **shall** be operationally realistic.

Reliability verification **shall** be an integral part of the overall system/product engineering verification and be coordinated and integrated across all phases. The customer may have specific test requirements (e.g., reliability qualification testing, testing in customer facilities, customer-controlled, customer-scored testing). The customer may choose to review and approve the verification strategy/plan.

5.5.1.10 Failure Definitions and Scoring

The developer **shall** design the system/product to meet reliability requirements when the failure definitions and scoring criteria identified in Section 4.5.1.7 are used and the system/product is operated and maintained by the user. The developer **shall** identify and mitigate human errors, (excluding those due to deliberate maliciousness and/or obviously reckless use), that may occur when actual users operate and maintain the system/product.

5.5.1.11 Technical Reviews

The developer **shall** conduct technical interchanges with the customer/user as set forth in the Reliability Program Plan. The developer **shall** conduct formal reviews for reliability that promote an understanding of the user environment in which the system/product will operate and to assure progress toward achieving the reliability requirements as set forth in the Reliability Program Plan. An independent, detailed, peer review **shall** be conducted by impartial, objective individuals competent in the appropriate technical fields.

5.5.1.12 Methods and Tools

The developer **shall** implement the activities in Section 5.5.1 with appropriate reliability design and development methods and tools. Section 5.5.2 provides an overview of many such methods. The developer **shall** select appropriate methods and describe them in the updated Reliability Program Plan. The customer may elect to review, comment, and negotiate regarding the methods selected by the developer. The developer **shall** identify and employ a set of design-reliability best practices.

5.5.1.13 Outputs and Documentation

While executing the activities in Section 5.5.1, a number of outputs will be generated. In many cases, these outputs are inputs that are required by the other objectives in this standard. The developer **shall** document these outputs in an updated Reliability Case or equivalent documentation.

5.5.2 Methods and Tools (Informative)

In order to implement the activities in Section 5.5.1, a variety of reliability methods and tools will be needed. Some of the most popular methods and tools are listed in Annex A. A list of reliability best practices is provided in Annex B.

.

6 Objective 3: Produce Reliable Systems/Products

6.1 Introduction (Informative)

Once a system/product has been designed and developed, the next objective is to manufacture reliable copies. Imperfect quality during production can markedly reduce the design reliability of the system/product. The purpose of this objective is to ensure that systems/products are manufactured without appreciably degrading the reliability that was designed-in during the execution of Objective 2. Figure 4 graphically depicts the operation of this Objective.

6.2 Mission and Goals (Informative)

Manufacturing must be a controlled process that ensures that the systems/products provided to the user do not include manufacturing defects. During production, the developer organization seeks to build production units, demonstrate acceptable performance of these units, and have them pass acceptance testing without degrading the designed-in reliability levels of the system/product. The mission, then, is to maintain designed levels of reliability during production. All production systems/products (prototype, low-rate initial production, and full-rate production) must strive to meet the reliability requirements. Component choice, vendor choice, manufacturing technique, and system/product integration are all important considerations that must be closely monitored during production.

6.3 People and Organizations (Normative)

The performance of the reliability activities specified in Section 6.5.1 **shall** be an integral part of the system/product-engineering process. The developer shall ensure that the system /product continues to meet its inherent design reliability requirements during production, testing and field service. And, as a minimum, both a developer and customer reliability engineer **shall** be assigned to the multifunctional team. The developer **shall** document the management and organizational structure of those responsible for the performance of reliability activities in the updated Reliability Program Plan.

6.4 Supporting Information

As a minimum, the input information listed under Input Information below is needed in order to begin to produce reliable systems/products. Developed Information lists the information that will be developed as reliable systems/products are produced using the activities included under this objective.

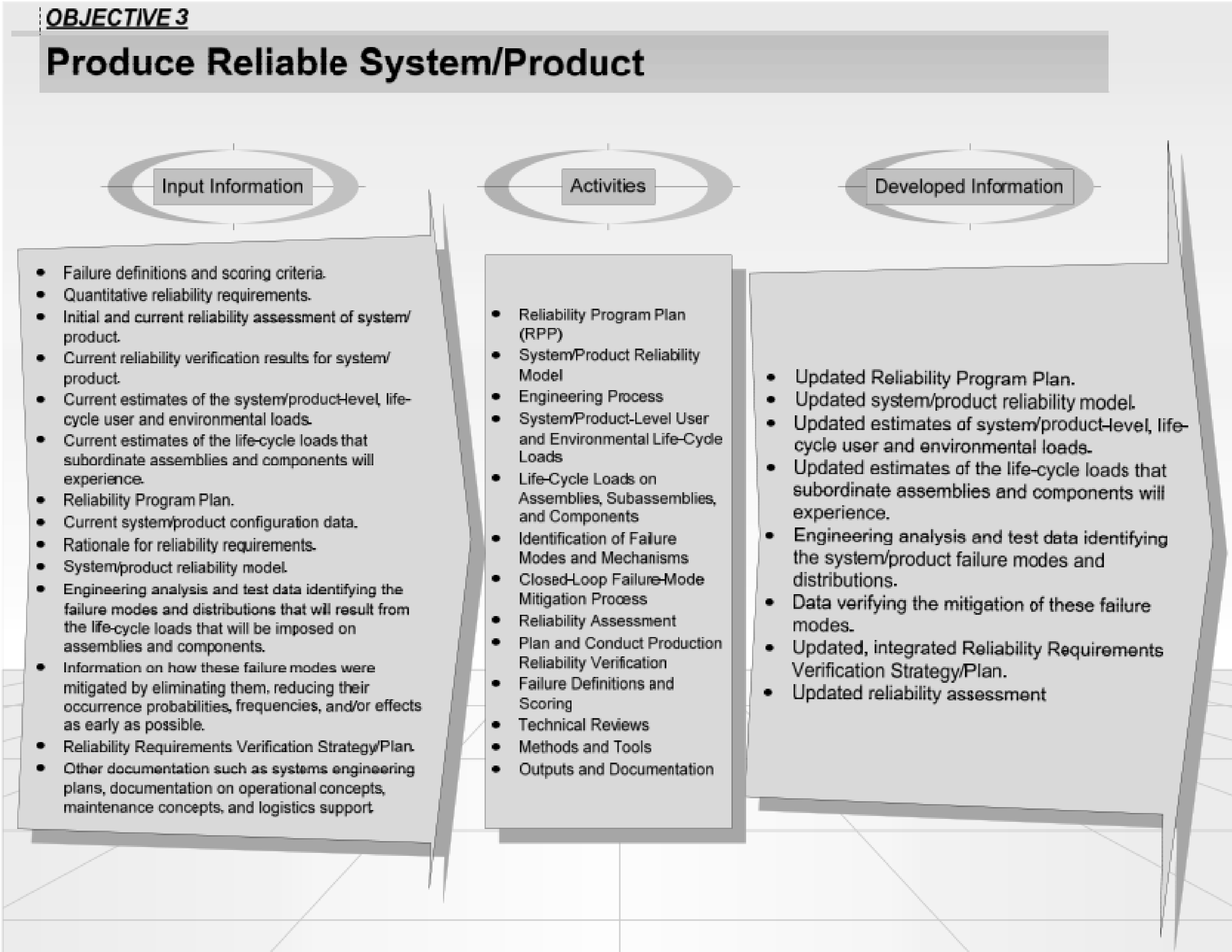

Figure 4 — Objective 3 Inputs, Activities, and Outputs

6.4.1 Input Information (Normative)

The following information is required before a reliable system/product can be produced:

- Failure definitions and scoring criteria.
- Quantitative reliability requirements.
- Initial and current reliability assessment of system/product.
- Current reliability verification results for system/product.
- Current estimates of the system/product-level, life-cycle user and environmental loads.
- Current estimates of the life-cycle loads that subordinate assemblies and components will experience.
- Reliability Program Plan.
- Current system/product configuration data.
- Rationale for reliability requirements.
- System/product reliability model.
- Engineering analysis and test data identifying the failure modes and distributions that will result from the life-cycle loads that will be imposed on assemblies and components.
- Information on how these failure modes were mitigated by eliminating them, reducing their occurrence probabilities, frequencies, and/or effects as early as possible.
- Reliability Requirements Verification Strategy/Plan.
- Other documentation such as system/product engineering plans, documentation on operational concepts, maintenance concepts, and logistics support.

6.4.2 Developed Information (Normative)

The activities described in Section 6.4.1 will result in this developed information. The information developed **shall** include:

- Updated Reliability Program Plan.
- Updated system/product reliability model.
- Updated estimates of system/product-level, life-cycle user, and environmental loads.
- Updated estimates of the life-cycle loads that subordinate assemblies and components will experience.
- Engineering analysis and test data identifying the system/product failure modes and distributions.
- Data verifying the mitigation of these failure modes.
- Updated, integrated Reliability Requirements Verification Strategy/Plan.
- Updated reliability assessment.

6.5 Activities, Methods, and Tools

This section is divided into two parts. The first part, Section 6.5.1, specifies the activities that the developer **shall** perform. The second part, Section 6.5.2, is informative in nature and lists methods and tools that the developer may consider to effectively support the activities in Section 6.5.1.

All activities, methods and tools used should be evaluated and applied in a manner that adds demonstrated value to the program, at an optimized life cycle cost and utilization of resources, in support of the stated mission and goals of this Objective.

6.5.1 Activities (Normative)

6.5.1.1 Reliability Program Plan (RPP)

The developer **shall** follow the current RPP in the performance of all activities in Section 6.5.1. Updates to reliability requirements and the RPP **shall** be recommended based on quantified and supporting rationale with customer involvement and approval.

6.5.1.2 System/Product Reliability Model

The developer **shall** update the system/product reliability model developed in Section 5.5.1.2, if necessary, based on any design changes that occur or as new, perhaps manufacturing- or quality-related failure modes are identified during production.

6.5.1.3 Engineering Process

The developer **shall**

1. incorporate the reliability activities as an integral part of a disciplined and documented systems and/or design engineering process and plan,
2. submit the potential reliability improvements identified during the execution of the reliability activities to the appropriate engineering organizations,
3. monitor and evaluate the reliability impact of changes to the design or manufacture of the system/product,
4. identify, manage, and control reliability-critical items, and
5. ensure adherence to design rules that impact reliability, including stress derating, electrical, mechanical, thermal, and other guidelines.

6.5.1.4 System/Product-Level User and Environmental Life-Cycle Loads

The developer **shall** periodically update the estimates of the life-cycle user and environmental loads developed in Section 5.5.1.4. These estimates **shall** be verified with measurements on production-representative systems/products or suitable substantiating data sources approved by the customer.

6.5.1.5 Life-Cycle Loads on Assemblies, Subassemblies, and Components

The developer **shall** update estimates developed in Section 5.5.1.5 of the life-cycle loads that subordinate assemblies, subassemblies, components, COTS, NDI, and CFI will experience as a result of the system/product-level user and environmental loads estimated in Section 6.5.1.4. These updates **shall** be provided to engineering teams responsible for developing and producing assemblies, subassemblies, and components for this system/product. These estimates **shall** also be provided to teams tracking and monitoring items not specifically developed for this system/product, which may include COTS, NDI, and CFI, as well as assemblies, subassemblies, and components. These updates **shall** be refined periodically as the system/product-level loads are updated, and/or as the design evolves. The teams that received initial estimates **shall** be provided with these updated estimates. Eventually, the estimates **shall** be verified with measurements (e.g., from instrumented production-representative systems/products).

6.5.1.6 Identification of Failure Modes and Mechanisms

The identification of failure modes and mechanisms specified in Section 5.5.1.6 **shall** continue during production as the design evolves and/or as the life-cycle load estimates in Section 6.5.1.5 are updated.

When systems/products are manufactured, variation in quantities such as geometric dimensions and material properties will occur. This manufacturing variation may introduce failure modes not previously identified or it may cause known failure modes to occur earlier in the life cycle. New or modified failure modes resulting from the impact of manufacturing variation **shall** be identified and confirmed through analysis, test, or accelerated test. Failure modes due to manufacturing process or workmanship errors **shall** be identified and confirmed in a similar fashion.

Failures that occur during either production testing or screening **shall** be analyzed until the root cause failure mechanism has been identified. Identification of the failure mechanism provides the insight essential to the identification of reliability improvements. Predicted failure modes/mechanisms **shall** be compared with those from test and the field.

6.5.1.7 Closed-Loop Failure-Mode Mitigation Process

The developer **shall** continue the failure-mode mitigation process specified in Section 5.5.1.7 throughout production. The developer **shall** aggressively mitigate failure modes until the reliability requirements are successfully verified.

6.5.1.8 Reliability Assessment

As provided in the Reliability Program Plan, the developer **shall** perform production reliability assessments. Formal reliability growth methodology **shall** be used where applicable (e.g., when failure modes are discovered and addressed with a test-analyze-and-fix process) in order to track and project reliability improvement.

6.5.1.9 Plan and Conduct Production Reliability Verification

The developer **shall** plan and conduct activities to ensure that the reliability requirements are met and maintained during production. The developer **shall** refine the Reliability Requirements Verification Strategy/Plan initiated under the first and second objectives. The verification **shall** be based on analysis, modeling & simulation, testing, or a mixture. Reliability verification **shall** be an integral part of the overall system/product verification and be coordinated and integrated across all phases. Testing **shall** be operationally realistic. The customer may have specific test requirements (e.g., reliability qualification testing, testing in customer facilities, or customer-controlled, customer-scored testing). The customer may choose to review and approve the verification strategy/plan.

6.5.1.10 Failure Definitions and Scoring

The developer **shall** develop the system/product to meet reliability requirements when the failure definitions and scoring criteria identified in Section 4.5.1.7 are used and the system/product is operated and maintained by the user. The developer **shall** identify and mitigate human errors, (excluding those due to deliberate maliciousness and/or obviously reckless use) that may occur when actual users operate and maintain the system/product.

6.5.1.11 Technical Reviews

The developer **shall** conduct technical interchanges with the customer/user. The developer **shall** conduct formal reviews for reliability that promote an understanding of the user environment in which the system/product will operate and to assure progress toward achieving the reliability requirements.

6.5.1.12 Methods and Tools

The developer **shall** implement the activities in Section 6.5.1 with appropriate reliability methods and tools. Section 6.5.2 provides an overview of many such methods. The developer **shall** select appropriate methods and describe them in the updated Reliability Program Plan. The customer may elect to review, comment and negotiate regarding the methods selected by the developer. The developer **shall** identify and employ a set of production-reliability best practices.

6.5.1.13 Outputs and Documentation

While executing the activities in Section 6.5.1, a number of outputs will be generated. In many cases, these outputs are inputs that are required by the other objectives in this standard. The developer **shall** document these outputs in an updated Reliability Case or equivalent documentation.

6.5.2 Methods and Tools (Informative)

In order to implement the activities in Section 6.5.1, a variety of reliability methods and tools will be needed. Some of the most popular methods and tools are listed in Annex A. A list of reliability best practices is provided in Annex B.

7 Objective 4: Monitor and Assess User Reliability

7.1 Introduction (Informative)

The fielding portion of the reliability continuum has a direct impact on total life cycle cost and affordability. Operation and support costs for an unsatisfactory level of design and/or process reliability can represent the majority of the total life cycle cost for a system or product. A robust reliability program that is sustained through the fielding phase of the life cycle can significantly reduce the operation and support cost associated with any major system or product. Figure 5 graphically depicts the operation of this Objective.

An effective reliability program requires both valid data, clear definitions of failure, and the identification of those data elements that support monitoring and assessment of system/product reliability. The reliability analyses and assessments performed and/or updated during the field phase of the system/product life cycle must be directly linked to those performed during all previous life cycle phases. For a well-defined and robust reliability program, the parameters that are assessed once the system/product is in the field will facilitate continued and effective reliability growth, as well as provide metrics that can be used to validate reliability assessments that were performed in earlier phases of the life cycle. This continuous assessment, developed through a robust closed feedback loop throughout the enterprise, provides an excellent means to compile lessons learned and improve both current and future reliability programs.

7.2 Mission and Goals (Informative)

The mission of this Objective is to establish and execute the requirements of a field reliability monitoring system, comprising data collection, analysis, maintenance, and closed-loop feedback activities, that maximize the confidence that the inherent design and/or process reliability of the fielded product are not degraded by field activities; that the inherent design and/or process reliability of the fielded product continue to grow based on investigation into, and elimination of, root failure causes in the design and/or related processes; that any new system/product failure mode experienced in the field that has not been previously accounted for in reliability analyses or testing is documented and communicated to all cognizant personnel for investigation and mitigation of root failure cause; and that all reliability data collected from the field is traceable to specified system/product reliability requirements and their metrics.

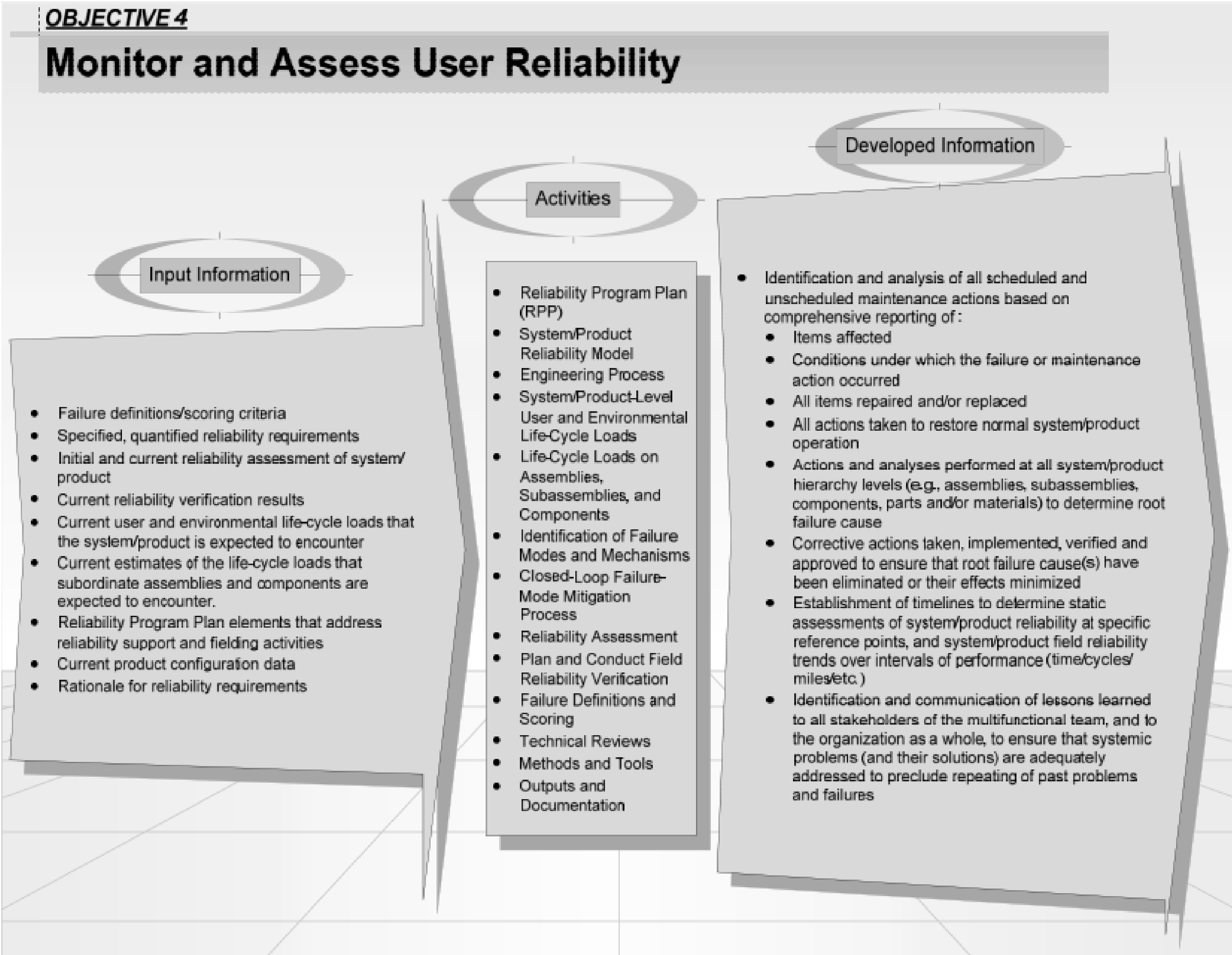

Figure 5 — Objective 4 Inputs, Activities, and Outputs

7.3 People and Organizations (Normative)

The multifunctional team that was established during the earlier development phases of the product life cycle may evolve as the life cycle progresses, but a multifunctional team **shall** continue to be staffed to support the mission and goals of this Objective. Staffing should include representatives from organizations such as Program Management; Systems and/or Design Engineering (to include Reliability Engineering); Manufacturing and/or Process Engineering; Quality Assurance/Control; and Field Maintenance/Support operations. While individual stakeholders on the team and team members may change over program phases, the program **shall** maintain continuity of resources, skills, and assets throughout the life-cycle phases of the program.

The Lead for the multifunctional team should represent the organization (e.g., the Program Manager for DoD) that is most responsible for the reliability of the system/product in the field. Accountability **shall** be assigned to all members of the team to support the mission and goals of this Objective.

7.4 Supporting Information

As a minimum, the input information listed under Input Information below is needed in order to begin to monitor and track field performance. Developed Information lists the information that will be developed as data is reported and analyzed from the field using the activities included under this objective.

7.4.1 Input Information (Normative)

All data and information that is defined, collected, and analyzed during the fielding phase of the system/product life cycle **shall** be compatible with the requirements and reliability program activities associated with the previous life cycle phases. This compatibility requires that the data and information **shall** be traceable to the satisfaction of specified reliability technical and program requirements and supporting metrics. The collected data/information **shall** directly support the update of previously performed assessments and analyses in both content and format.

Inputs to this Objective from previous life cycle phases **shall** include:

- Failure definitions/scoring criteria
- Specified, quantified reliability requirements
- Initial and current reliability assessment of system/product
- Current reliability verification results
- Current estimates of user and environmental life-cycle loads that the system/product will encounter
- Current estimates of the life-cycle loads that subordinate assemblies and components will encounter
- Reliability Program Plan elements that address reliability support and fielding activities
- Current product configuration data
- Rationale for reliability requirements

Additional information and data supporting the configuration of the items being monitored for reliability may come from system/product configuration data (i.e., part or serial number control); bills of materials (BOMs); component and software libraries; FMEA/FMECA results; reliability predictions; reliability centered maintenance (RCM) results; failure reporting, analysis and corrective action systems (FRACAS); reliability-critical items lists (CILs); test results (accelerated life, reliability growth, reliability demonstration, etc.); statistical life data analysis (Weibull analysis, Monte Carlo simulations, etc.); physics-of-failure analysis; Design of Experiments; lessons learned databases; etc.

7.4.2 Developed Information (Normative)

All outputs and documentation generated as a result of this Objective **shall** directly or indirectly support and be traceable to specified reliability requirements and metrics. All outputs, documents, data, and information generated as part of this Objective **shall** be analyzed and applied in a manner that will ensure that the inherent reliability of the fielded system/product design will not be degraded by maintenance actions, processes or procedures, or change in production or quality, and that failures experienced in the field result in corrective action(s) that continue to improve and grow the reliability of the product in a cost- and resource-optimized manner.

As a minimum, outputs and documentation generated and communicated during this phase of the system or product life cycle **shall** facilitate:

1. Identification and analysis of all scheduled and unscheduled maintenance actions based on comprehensive reporting of :
   a. Items affected
   b. Conditions under which the failure or maintenance action occurred
   c. All items repaired and/or replaced
   d. All actions taken to restore normal system/product operation
   e. Actions and analyses performed at all system/product hierarchy levels (e.g., assemblies, subassemblies, components, parts, and/or materials) to determine root failure cause
   f. Corrective actions taken, implemented, verified, and approved to ensure that root failure cause(s) have been eliminated or their effects minimized
2. Establishment of timelines to determine static assessments of system/product reliability at specific reference points, and system/product field reliability trends over intervals of performance (time/cycles/miles/etc.)
3. Identification and communication of lessons learned to all stakeholders of the multifunctional team, and to the organization as a whole, to ensure that systemic problems (and their solutions) are adequately addressed to preclude repeating of past problems and failures

Outputs and documentation may be generated and made available in either hardcopy, electronic, or web-based formats, but an integrated and centralized reporting and closed-loop communication process and system **shall** be established, if not already defined and implemented in previous Objectives of this standard. The process/system developed from previous life cycle phases **shall** be utilized if it remains sufficient for the fielding phase, as agreed to by the customer and the developer. This process/system **shall** allow controlled access by all relevant multifunctional team stakeholders. Additionally, the closed-loop process/system **shall** be capable of capturing all review and approval signatures at appropriate levels within the organization to ensure a rigorous approach to the identification, resolution, and correction of design, process, or procedural failures that inhibit the sustainment or growth of current and future system/product reliability.

7.5 Activities, Methods and Tools

This section is divided into two parts. The first part, Section 7.5.1, specifies the activities that the developer **shall** perform. The second part, Section 7.5.2, is informative in nature and lists methods and tools that the developer may consider to effectively support the activities in Section 7.5.1.

All activities, methods, and tools used should be evaluated and applied in a manner that adds demonstrated value to the program, at an optimized life cycle cost and utilization of resources, in support of the stated mission and goals of this Objective.

7.5.1 Activities (Normative)

The activities under this Objective **shall** support the stated missions and goals of the overall reliability program. Corrective action based on the activities performed as part of this Objective **shall** be implemented in the system/product design and processes to ensure that both long term reliability growth trends are sustained and total life cycle cost (TLCC) is optimized. As an example, an update to a FMEA/FMECA would be considered a value-added activity if it

1. results in a design or process change that improves system/product reliability and
2. reduces TLCC based on implementation of the FMEA/FMECA results.

The activities performed under this Objective **shall** be performed to:

1. Track, monitor, assess, and improve system/product reliability during the fielding portion of its life cycle to ensure that inherent reliability performance is sustained
2. Ensure that all field-measured reliability metrics are directly traceable to, and compatible with:
   a. Specified reliability requirements
   b. Previous reliability assessments and analyses, such as failure modes and effects analysis (FMEA), failure modes, effects, and criticality analysis (FMECA), reliability assessments, reliability tests, failure trend analysis, etc.
3. Identify root causes of hardware, software, human factor, and/or process and procedural failures that are identified as part of both unscheduled and scheduled system/product maintenance actions
4. Discriminate between true root failure causes and symptom-related failure causes that, when corrected, may temporarily restore system/product operation, but mask the true root failure cause
5. Collect and feed back actionable data and information to multifunctional team stakeholders that will result in the identification, implementation, assessment, and verification of corrective actions that eliminate or minimize root failure cause effects. Actionable data/information may include, but not be limited to:
   a. The determination of individual and cumulative system or product timelines to correlate accumulated life units (hours/cycles/miles/etc.) to unscheduled maintenance or failure events
   b. Normal environmental and user profile conditions that existed when the failure occurred, or leading up to when the failure occurred

   c. Anomalies in environmental and user profile conditions that existed when the failure occurred, or leading up to when the failure occurred
   d. Identification of the characteristics of the failure, including intermittency and/or quantified performance degradation, and how system/product performance was ultimately affected
6. Ensure that the assessment of field failures, particularly for the purposes of measuring reliability performance or determining root failure cause, are based on the contractual definition of failure and failure scoring criteria over the system/product life cycle. Definitions of failure **shall** describe those specific, quantifiable, and measurable conditions and scoring criteria that constitute a relevant failure, a non-relevant failure and, for degradation failures, the threshold of performance degradation allowed before a failure is declared.
7. Corrective actions that result from analysis of the collected data and information are identified, implemented, and verified as being effective (through test or analysis) in improving the reliability of the fielded product.

7.5.1.1 Reliability Program Plan (RPP)

The developer **shall** follow the current RPP in the performance of all activities in Section 7.5.1. Updates to reliability requirements and the RPP **shall** be recommended based on quantified and supporting rationale with customer involvement and approval.

7.5.1.2 System/Product Reliability Model

The developer **shall** update the system/product reliability model refined in Section 6.5.1.2, if necessary, based on any design changes that result from field failures, such as those that may result when new, unexpected failure modes are identified.

7.5.1.3 Engineering Process

The developer **shall**

1. incorporate the reliability activities as an integral part of a disciplined and documented systems and/or design engineering process and plan,
2. submit the potential reliability improvements identified during the execution of the reliability activities to the appropriate engineering organizations,
3. monitor and evaluate the reliability impact of changes to the design or manufacture of the system/product,
4. identify, manage, and control reliability-critical items, and
5. ensure adherence to design rules that impact reliability, including stress derating, electrical, mechanical, thermal, and other guidelines.

7.5.1.4 System/Product-Level User and Environmental Life-Cycle Loads

The developer **shall** update the life-cycle user and environmental load estimates developed in Section 6.5.1.4 based on actual environmental and failure data collected during field operations, or changes in environmental profiles brought about by new applications of the system/product not previously defined by existing requirements.

7.5.1.5 Life-Cycle Loads on Assemblies, Subassemblies, and Components

The developer **shall** update estimates from Section 6.5.1.5 of the life-cycle loads that subordinate assemblies, subassemblies, components, COTS, NDI, and CFI will experience as a result of the system/product-level user and environmental loads estimated in Section 7.5.1.4. These updates

shall be provided to the engineering teams responsible for developing assemblies, subassemblies, and components for this system/product. These updates **shall** also be provided to teams tracking and monitoring items not specifically developed for this system/product, which may include COTS, NDI, and CFI, as well as assemblies, subassemblies, and components.

7.5.1.6 Identification of Failure Modes and Mechanisms

The identification of failure modes and mechanisms are critical activities of this Objective, both to verify that previous reliability assessments and analyses have accurately identified those modes/mechanisms that are expected and being experienced in the field, and to ensure that previously unidentified modes/mechanisms are fed back into the process to update previous assessments and analyses.

Failures that occur in the field **shall** be analyzed, as appropriate to optimize safety, reduce risk, and optimize TLCC, until the root failure cause, mode, and mechanism have been identified. This activity provides the insight essential to the identification of reliability improvements through verified/approved corrective actions. Failure modes/mechanisms identified through previous analyses **shall** be compared to those from field operation and the analyses updated accordingly.

7.5.1.7 Closed-Loop Failure Mode Mitigation Process

The developer **shall** use an integrated team that includes suppliers of assemblies, subassemblies, components, and selectors/integrators COTS, NDI, and CFI, as necessary to determine true root failure cause and analyze all failure modes arising from field operations in order to formulate verifiable corrective actions for approval.

Failure modes **shall** be addressed and resolved in a timely manner consistent with
1. the criticality of their impact on safety, reliability, and performance requirements and
2. their impact on the TLCC of the system/product.

Failure modes **shall** be mitigated by one or more of the following approaches:
- Eliminating the failure modes
- Reducing their occurrence probabilities or frequencies
- Incorporation of redundancy
- Mitigation of failure effects (e.g., fault recovery, degraded modes of operation, providing advance warning of failure).

The developer shall aggressively mitigate failure modes in order to keep reliability from degrading in the field.

The developer **shall** employ methods and tools for monitoring and communicating, throughout the organization (and to suppliers, as appropriate):
1. descriptions of field incidents and failures,
2. analysis results identifying root-cause failure modes and mechanisms, and
3. the status of corrective actions and risk-mitigation decisions.

These methods and tools **shall** be made accessible to the customer.

Failure modes that are expected to occur during the system/product life cycle shall be included in the system/product reliability model.

7.5.1.8 Reliability Assessment

The developer **shall** update reliability assessments of the system/product throughout the fielding portion of the life cycle. Reliability estimates from analysis, modeling & simulation, and testing performed during previous life cycle phases **shall** be updated based on field experience and compared against customer reliability requirements. The implementation of corrective actions **shall** be verified and their effectiveness tracked. Formal reliability growth methodology **shall** be used where applicable (e.g., when new field failure modes are discovered in the field) in order to track and project reliability improvement.

7.5.1.9 Plan and Conduct Field Reliability Verification

The developer **shall** plan and conduct activities to ensure that reliability requirements will be met in the fielded environment. The developer **shall** provide feedback into the reliability verification process to support field reliability requirements. A customer may choose to review and approve the developer's activities to ensure that reliability requirements continue to be met in the fielded environment.

7.5.1.10 Failure Definitions and Scoring

The developer **shall** monitor and report on system/product reliability in the field based on the failure definitions and scoring criteria defined as part of the reliability requirements. The developer **shall** identify and mitigate hardware, software, process, and procedural failures, as well as human factor errors that may occur when users operate and maintain the product.

7.5.1.11 Technical Reviews

As set forth in the Reliability Program Plan, the developer **shall** conduct and participate in formal reviews for reliability that address the identification, analysis, classification, and resolution of hardware, software, process, procedural, or human factors failures that result from operation of the system/product in the field.

7.5.1.12 Methods and Tools

The developer **shall** support the activities defined in Section 7.5.1 with appropriate reliability data collection, analysis, and communication methods and tools. The developer **shall** ensure that the selected methods and tools are described in the RPP, and that the RPP is updated to reflect new tools and methods that may be introduced to improve the effectiveness and efficiency of the closed-loop failure mode mitigation process. The customer may elect to review, comment, and negotiate regarding the methods and tools being used by the developer.

7.5.1.13 Outputs and Documentation

While executing the activities in Section 7.5.1, a number of outputs (specified below in Outputs and Documentation) will be generated. In many cases, these outputs are inputs that are required by the other Objectives in this standard. The developer **shall** document these outputs in an updated Reliability Case or equivalent documentation.

7.5.2 Methods and Tools (Informative)

The information in this section is provided for guidance purposes only.

The basic intent of the methods and tools defined by this Objective is to implement a closed loop data and information system that **will**:

1. Support traceability of data and information to specified reliability requirements and metrics (i.e., do they correlate to requirements)
2. Provide data and information that explicitly or implicitly contributes to the satisfaction of specified reliability requirements (i.e., do they meet requirements)
3. Provide data to, and/or use data from, the technical and administrative feedback loops that are necessary to support continued reliability growth of the fielded system/product
4. Promote the identification, evaluation, understanding, and resolution of problems such that there is an overall positive impact on the reliability of systems/products in the field through redesign efforts or process/procedural changes
5. Facilitate the sharing of data, information, and results between stakeholders on the multifunctional team (including the customer and lower-tier suppliers), and throughout the organization as a whole

In order to implement the activities of Section 7.5.1, a variety of reliability methods and tools should be considered. Some of the most popular methods and tools supporting this Objective are listed in Annex A. A list of reliability best practices is provided in Annex B.

7.6 Outputs and Documentation (Normative)

While executing the activities of Section 7.5.1, a number of outputs will be generated. In many cases, these outputs are inputs that **shall** be fed back as inputs to previous Objectives of this standard, for the purposes of

1. updating reliability requirements that are proven to be incorrect or obsolete (Objective 1),
2. facilitating design, process, or procedural modifications that will improve the design of current or future products (Objectives 2 and 3), and
3. quantitatively supporting reliability re-verification based on design, process, or procedural modifications (Objectives 2 and 3).

Additionally, these outputs will be needed in order to update the Reliability Case and provide progressive assurance to the customer that reliability requirements will continue to be met.

Potential outputs are:

- Modifications to the Reliability Program Plan.
- Updated system/product reliability model.
- Updated system/product-level life-cycle user and environmental loads.
- Updated estimates of the life-cycle loads that subordinate assemblies and components will experience.
- Information verifying the failure modes and mechanisms identified during previous life-cycle phases, or identifying new failure modes and mechanisms not previously identified.

- Information on how root failure causes and their associated failure modes were addressed by eliminating them, or reducing their occurrence probabilities, frequencies, and/or effects as early as possible to optimize safety and TLCC.
- Updated reliability analyses and assessments.
- Updated Maintenance Plans and Logistics Support Structure.

The outputs **shall** be documented in an updated Reliability Case or equivalent documentation.

Annex A – Methods Matrix (Informative)

The methods listed in the matrix below are those items typically performed over the system's/product's life cycle that have an impact on the total life cycle cost during design, development, production, delivery, and support of a system/product. These methods enable the system/product design to be more reliable (fewer failures) and more maintainable (fewer resources needed) and the total life cycle cost for the system/product will be lower.

The following terminology is used in the matrix:

- Method: The name of a process or analysis used to develop a robust, reliable design.
- Reference: The document number that contains a detailed description of method.
- Product Phase: A product design, delivery, or support phase where a particular method is applicable. This ● symbol denotes that the method is a primary contributor in the product phase. The Δ symbol denotes that the method is used as needed or is updated with available product data.
- Product Phase Objective 1: Understand customer/user requirements and constraints. This phase focuses on focuses on the development of reliability requirements and metrics, pre-acquisition activities, design concepts and design trade studies. Objective 1 tasks consists of the Design Concept tasks, which evaluate the contractual documents and specifications for candidate design options that will support the user's/customer's life cycle cost goals; and Design Trades that provide the customer and developer with the opportunity for early refinement and possible down-select of multiple design options.
- Product Phase Objective 2: Design and redesign for reliability. This phase focuses on successful approaches for designing-in reliability. Objective 2 tasks consist of the Preliminary Design Review to validate that the initial system/product design is capable of meeting the reliability requirements; Prototype Test and Evaluation that provide confirmation that the design is capable or identifies areas for potential redesign; and the Critical Design Review incorporates the findings of the Preliminary Design Review and the Prototype Test and Evaluation to establish the final design configuration.
- Product Phase Objective 3: Produce reliable systems/products. This phase focuses on the production reliability starting with limited production. Objective 3 tasks consists of the Demonstration and Qualification of the system/product which provides the body of evidence that the reliability requirements have been achieved and the design is fully capable of meeting the customer's/user's needs. The Final Design incorporates all outstanding design issues, additional design concerns from the design demonstrations and qualification testing and any manufacturing process changes needed in preparation for the low rate initial production and full rate production. Objective 3 culminates with Production delivery of a proven system/product to the user/customer.

- Product Phase Objective 4: Monitor and assess user reliability. This phase focuses on monitoring and managing reliability once the system/product in the hands of the user. While the developer strives for "perfect parts and prefect processes" design deficiencies will be surfaced through on-going production testing and system/product usage by the user. The developer's Change Control Process is key to the continued "as designed" performance of the system/product and preventing reliability margin erosion. Once the design has been released and under formal Change Control, design changes are made to correct design errors found during deployment, improve manufacturing assembly and reduce manufacturing cost. Changes evaluated on an individual basis typically are not significant reliability drivers, but collectively, these changes can adversely impact the design reliability analysis. Operation and Delivery data collection is needed to further correct design deficiencies uncovered by the user under actual use conditions that can not be replicated by the developer, and Delivery and Maintenance data collection through factory and depot repairs provides the needed data to assess the long term system/product field reliability assessments.

References denoted as DoD guidance in the table below can be found in the DoD RAM Guide, available for download at http:// www.acq.osd.mil/sse/docs/**RAM_Guide**_080305.pdf or by contacting OUSD(AT&L) DS/SE/ED via ATL-ED@OSD.MIL.

The information in this section is provided for guidance purposes only and is not intended to be an all inclusive list.

Method [Reference]	**Product Phase**										
	Objective 1		**Objective 2**			**Objective 3**			**Objective 4**		
	Design Concept	**Design Trades**	**Preliminary Design Review**	**Prototype Test & Evaluation**	**Critical Design Review**	**Design Demonstration and Qualification**	**Final Design**	**Production**	**Change Control Process**	**Operation & Delivery**	**Delivery and Maintenance**
Accelerated Testing Methods (such as TAFT, RDGT, HALT, ALT) [DoD 4.5.2.16, SAE JA1000-1 A.1]		•	•	•	•	•		Δ			
Bayesian Techniques [DoD 4.5.2.29]	•	•	•							Δ	Δ
Benchmarking [DoD 4.5.2.12]		•									
Block Diagram Development [SAE JA1000-1 A.2]	•	•	•	•							
Capability Maturity Model Integration (CMMI) Software Engineering Institute/Carnegie Mellon			•	•	•	•	•	•	•	•	•
Commercial-Off-the-Shelf (COTS) Assessment [DoD 4.5.2.20]	•	•	•	•	•			Δ	Δ		
Component Testing [DoD 4.5.2.18]		•	•	•	•	•		•	Δ		
Condition Based Maintenance (CBM) [DoD 6.5.8]					•	•	•				

Method [Reference]	Product Phase										
	Objective 1		Objective 2			Objective 3			Objective 4		
	Design Concept	Design Trades	Preliminary Design Review	Prototype Test & Evaluation	Critical Design Review	Design Demonstration and Qualification	Final Design	Production	Change Control Process	Operation & Delivery	Delivery and Maintenance
Critical Items List [DoD 3.5.6]			•		•		•	•	Δ		
Data Collection, Analysis and Corrective Action System (DCACAS) [DoD 4.5.2.7]			•	•	•	•	•	•	•	•	•
Data Management Technique (PREDICT) [DoD 4.5.2.8]			•	•	•	•	•	•	•	•	•
Design for Manufacturing and Design for Assembly [SAE JA1000-1 A.3]	•	•	•	•	•	•	•		Δ		
Design of Experiments (Classical) [SAE JA1000-1 A.4]	•	•	•	•	•				Δ		
Design of Experiments (Taguchi) [SAE JA1000-1 A.5]	•	•	•	•					Δ		
Design Guidelines for Reliable Surface Mount Technology Printed Board Assemblies [IPC-D-279]		•	•	•	•		Δ	Δ	Δ		
Design Review [SAE JA1000-1 A.6]	•		•		•		•		•		
Durability Analysis (Low Cycle, High Cycle, Strength of Materials, Solder Joint) [DoD 6.5.1.4]			•	•	•	Δ	Δ		Δ		
Durability Verification Test [DoD 1.4.5.1]						•	Δ				
Environmental and Product Usage Profile /Mission Profile [DoD 4.5.2.2, SAE JA1000-1 A.7]	•	•	•	•	•	•	•	Δ	Δ	Δ	Δ
Environmental Qualification Test [DoD 5.5]						•					
Environmental Stress Screening (ESS)/Highly Accelerated Stress Screening (HASS) [DoD 4.5.2.33, SAE JA1000-1 A.8]			•	•	•	•	•	•			
Error/Mistake Proofing [SAE JA1000-1 A.9]		•	•	•	•	•	•	•	Δ		Δ
Failure Modes and Effects Analysis (FMEA)/Failure Modes Effects and Criticality Analysis (FMECA) [DoD,SAE JA1000-1 A.10 and GEIA-STD-0007]		•	•	•	•	•	•	•	Δ		Δ
Failure Reporting Analysis and Corrective Action System (FRACAS) [SAE JA1000-1 A.11]			•	•	•	•	•	•	•	•	•

Method [Reference]	Product Phase										
	Objective 1		Objective 2			Objective 3			Objective 4		
	Design Concept	Design Trades	Preliminary Design Review	Prototype Test & Evaluation	Critical Design Review	Design Demonstration and Qualification	Final Design	Production	Change Control Process	Operation & Delivery	Delivery and Maintenance
Fault Insertion Testing [DoD 4.5.2]				•		•			Δ		
Fault Tree Analysis [DoD 4.5.2.10, SAE JA1000-1 A.13]		•	•	•	•	•	•	•	Δ		Δ
Focus Groups [SAE JA1000-1 A.15]	•	•	•	•							
General RAM Design Considerations [DoD 4.5.2.1]	•	•	•	•	•	Δ	Δ	Δ	Δ		
Ishikawa Diagram [DoD 4.5.2.11]		•		•							
Maintainability Demonstration (MDT) [DoD 4.5.2.23]						•	•	•	Δ	•	
Man-in-the-Loop Testing [DoD 4.5.2.23]				•	•						
Markov Modeling/Analysis [DoD 4.5.2.6, SAE JA1000-1 A.12]	•	•	•	•						•	•
Measurement Information Models Software Engineering Institute/Carnegie Mellon			•	•	•	•	•	•	•	•	•
Measurement Systems Analysis [SAE JA1000-1 A.16]				•	•	•		•			
Mission Profile Definition [DoD 4.5.2.2]	•	•	•								
One Shot Device Testing [DoD 4.5.2.32]		•		•		•		•	Δ		
Pareto Analysis [SAE JA1000-1 A.18]			•	•	•	•	•	•		•	•
Part Derating [SAE JA1000-1 A.42 JA1000-1 A.19]			•		Δ	Δ	Δ	Δ	Δ		
Parts Obsolescence and Diminishing Manufacturing Sources (DMSMS) [DoD 4.5.2.28]		•	•		•		•	•	•	•	•
Parts, Materials, Process Review/Control [SAE JA1000-1 A.20]	•	•	•		Δ		Δ	Δ	Δ		
Physics of Failure [DoD 4.5.2.14]		•	•	•	•	•	•	•	•	•	•
Practical Software Measurement Process Software Engineering Institute/Carnegie Mellon			•	•	•	•	•	•	•	•	•
Probabilistic Design – Stress and Strength Interference Method		•	•	•	•	•	•				

Method [Reference]	Product Phase										
	Objective 1		Objective 2			Objective 3			Objective 4		
	Design Concept	Design Trades	Preliminary Design Review	Prototype Test & Evaluation	Critical Design Review	Design Demonstration and Qualification	Final Design	Production	Change Control Process	Operation & Delivery	Delivery and Maintenance
[SAE JA1000-1 A.21]											
Process Failure Modes Effects Analysis / Producibility Analysis (PFMEA/PFMECA) [DoD and SAE JA1000-1 A.10]						•	•	•	Δ		
Production Process Capability Study [SAE JA1000-1 A.22]		•	•	•	•		•				
Program Parts Selection List [DoD 3.5.6]			•	Δ	Δ	Δ	Δ	Δ	Δ	Δ	
Pugh Selection [SAE JA1000-1 A.23]	•	•	•	•							
Quality and Quality Control [DoD 5.5.13]			•	•	•	•	•	•	•	•	•
Quality Function Deployment [SAE JA1000-1 A.24]	•	•	•	•							
Quality Loss Function [SAE JA1000-1 A.25]	•	•	•	•					Δ		
RAM Design Guide [DoD 3.5.6]			•								
Regression Analysis/Correlation/Prediction Modeling [DoD 4.5.2.13, SAE JA1000-1 A.26]				•		•		Δ		Δ	Δ
Reliability Allocation [DoD 3.5.6, SAE JA1000-1 A.27]	•	•	•	Δ	Δ	Δ	Δ		Δ		
Reliability Assessment [DoD 4.5.2.4]	•	•	•	Δ	•	Δ	•		Δ	•	•
Reliability Benchmarking [DoD 4.5.2.12, SAE JA1000-1 A.28]		•	•	•		•			Δ		
Reliability Case [DoD 3.5.7, SAE JA1000 Series, Def Stan 00-42, Part 3]	•	•	•	•	•	•	•	•	•	•	•
Reliability Centered Maintenance [DoD 4.5.2.21, SAE JA1011, SAE JA1012]			•		•		•			•	•
Reliability Demonstration Testing [DoD 4.5.2.31, SAE JA1000-1 A.30]						•	•	•	Δ		
Reliability Growth Modeling and Testing [DoD 4.5.2.15, SAE JA1000-1 A.31]			•	•	•	•		Δ	Δ	Δ	Δ
Reliability Growth Testing and Test-Analyze-Fix-Test (TAFT) [DoD 4.5.2.15]				•							

Method [Reference]	Product Phase										
	Objective 1		Objective 2			Objective 3			Objective 4		
	Design Concept	Design Trades	Preliminary Design Review	Prototype Test & Evaluation	Critical Design Review	Design Demonstration and Qualification	Final Design	Production	Change Control Process	Operation & Delivery	Delivery and Maintenance
Reliability Modeling and Prediction (Operating & Non-Operating) [DoD 4.5.2.5, SAE JA1000-1 A.32]	•	•	•	•	•	•	•	Δ	Δ	Δ	Δ
Reliability Program Plan [DoD 4.5.2.12]	•	•	•	•	•	•	•	•	•	•	•
Reliability Testing for Engineering Development, Qualification and Production [MIL-HDBK-781]				•	•	•	•	•			
Repair Strategy [DoD 4.5.2.3]	•	•	•	•	•	•	•	Δ	Δ	Δ	Δ
Repairable Systems Modeling/Analysis [DoD 4.5.2.19]	•	•	•	•	•	•	•	Δ	Δ	Δ	Δ
Requirements and Architecture Development [DoD 3.5.6]	•	•	•		•		•		Δ		
Risk Assessment [SAE JA1000-1 A.33]	•	•	•	•	•	•	•	•	•	•	•
Root Cause Analysis [SAE JA1000-1 A.34]			•	•	•	•	•	•	•	•	•
RQT and Acceptance Testing [DoD 4.5.2.31]						•					
Sampling Procedures [SAE JA1000-1 A.35]							•	•	Δ	Δ	Δ
Simulation (Markov Analysis) [DoD 4.5.2.6]	•	•	•		•	•			Δ	Δ	Δ
Simulation (Warranty) [DoD 5.5.2]		•	•		•		•	•			•
Sneak Circuit Analysis/Sneak Path Analysis [SAE JA1000-1 A.36]			•		•	Δ	Δ		Δ		
Software Reliability Growth Models Software Engineering Institute/Carnegie Mellon				•	•	•	•		Δ	Δ	Δ
Sparing Models Assessment Methods [DoD 5.5.2]			•	•	•	•	•				
Specification Generation (RAM requirements) [DoD 3.2.2]			•		•		•		Δ		
Statistical Process Control [SAE JA1000-1 A.37]			•	•	•	•	•	•	Δ		•
Surveys/Market Analysis [SAE JA1000-1 A.38]	•	•	•								
Testability Analysis (BIT/Diagnostics/Prognostics)			•	•	•	•	•	Δ	Δ	Δ	Δ

Method [Reference]	Product Phase										
	Objective 1		Objective 2			Objective 3			Objective 4		
	Design Concept	Design Trades	Preliminary Design Review	Prototype Test & Evaluation	Critical Design Review	Design Demonstration and Qualification	Final Design	Production	Change Control Process	Operation & Delivery	Delivery and Maintenance
[DoD 3.5.2.23, DoD 3.5.2.24]											
Warranty Tracking and Information Collection [SAE JA1000-1 A.40]							●	●		●	●
Worst Case Analysis [SAE JA1000-1 A.42]			●		●		Δ		Δ		

Annex B – Reliability Best Practices List (Informative)

The information in this section is a synopsis of the "Reliability of US Army Material Systems" memorandum, dated 6 December 2007, issued by Mr. Claude Bolton, Assistant Secretary of the Army for Acquisition, Logistics and Technology. This memorandum highlighted a number of systems that are failing to demonstrate established reliability requirements during operational testing and many are falling short of their established reliability requirement. This synopsis identifies systemic issues that the customer and developer can use to identify if the system/product is at risk of not meeting the reliability requirements and possible approaches to avoid potential pitfalls. These "reliability best practices" are not meant to be prescriptive but rather more informative with regard to what has contributed to a reduction in reliability performance.

Best Practice	Description
Build the Reliability Case	The developer routinely builds and updates a Reliability Case during product development. The Reliability Case documents the developer's understanding of the reliability requirements, the plan to achieve the requirements, and regularly-updated analysis of progress towards meeting the requirements. The Reliability Case provides the Customer assurance that the contractor is aggressively pursuing design practices and testing activities consistent with industry high performers.
Conduct Design Reviews	The developer conducts routine technical assessments of each reliability parameter based on the current known design configuration and knowledge throughout the product development cycle with a major emphasis on early assessments through technical reviews (technical reviews are typically design reviews such as System Requirements Review, System Functional Review, Preliminary Design Review, Critical Design Review, and Test Readiness Reviews as a minimum).
Conduct Technical Interchanges	The developer understands the rationale for the customer's reliability and maintainability requirements and conducts routine technical interchanges throughout the product development in order to understand and mature the customer's failure and maintenance definitions and scoring criteria based on the developer's latest detailed design configuration of the system.
Early Design Tests	The developer conducts early design testing that is specifically designed to precipitate failures so that the design can be improved early in the product design cycle.
Embedded Diagnostics	The developer has considered embedded instrumentation per CJCSI 3170.01F by incorporating diagnostics, prognostics, testing, and training into the product design early in the product development process and has assessed a number of options to include time-history based prognostics, precursor-based prognostics, and stress-history based prognostics.
Failure Mechanisms	The developer knows what the reliability challenges are and knows what the likely failure mechanisms and failure sites will be.
FMECA and Reliability Growth	The developer uses reliability engineering and management tools like Failure Modes and Effects Criticality Analysis (FMECA) and Reliability Growth techniques. It is critical that these tools and analyses be directly linked to the product design team. A developer may perform these reliability tasks but not use those results to influence the product design and to focus the product design team efforts. It is recommended that failure rate estimates, based on actual hardware test results, be used

Best Practice	Description
	as when available, in lieu of Handbook predictions in the FMECA for a more accurate assessment of the failure mode criticality.
FRACAS	The developer has a closed-loop Failure Reporting Analysis And Corrective Action System (FRACAS). The FRACAS process must be well structured and directly tied into the product design team. The FRACAS process must collect all of the information necessary to track and correct deficiencies. The FRACAS process should be under the purview of a failure review board that has the authority and commitment to assign resources to resolve problems.
HALT/HASS	The developer conducts Highly Accelerated Life Testing (HALT) and Highly Accelerated Stress Screening (HASS). The developer uses the lessons learned and the FMECA data to eliminate known failure modes. HALT is a strategy that is used to verify that the known failure modes have been eliminated and identify as many relevant failure mechanisms as possible in a relatively short time period using very small sample sizes. This strategy permits corrective actions to be made to strengthen the design and improve manufacturing processes early in the product development process before necessary program resources are exhausted. Corrective actions need to be identified and implemented in a timely manner for those design weaknesses that adversely impact the reliability.
Lean, Six Sigma	The developer understands the government's business transformation framework using Lean, Six Sigma and further understands and applies the Design for Lean, Six Sigma logic, tools, rigor, and discipline, System Engineering, and Supportability Engineering.
Lessons Learned	The developer has a well established and documented reliability and quality lessons learned.
Life Cycle Environment and Operational Duty Cycle	The developer must characterize the critical loads and stresses. A good design team will characterize the life cycle environment and operational duty cycle stresses that the product will be exposed to. This may require additional testing and data collection. Without knowing the environment that a product will operate in, or at least some reasonable bounds for the product's usage environment, the developers design team cannot be confident that the product will be reliable.
Life Limited Components	The developer has identified all the life-limited components. A cost effective replacement policy has been formulated for these components to maintain an adequate level of reliability throughout the product's lifecycle.
Low Level Testing and Integration Testing	The developer routinely conducts low-level testing starting very early in the product development process. The developer also conducts significant integration testing. The developer should routinely present the results, along with the results of the failure mechanism modeling, to the customer to demonstrate and provide progressive assurance that the product development is on a track that meets the specified reliability requirements.
MTBF vs. Failure Free Operation	The developer does not view reliability as just Mean Time Between Failure (MTBF). Instead the developer is focused on designing and building a product that has a significant failure-free operating period. The developer should address probabilistic analysis as part of the product design.
Nondeterministic Analysis and Probabilistic Technology	The developer understands and applies Nondeterministic Analysis and Probabilistic Technology to: product design, Systems Engineering and Supportability Engineering. The developer understands the implications of "uncertainty on decision-making" and assures quantification and

Best Practice	Description
	accountability to preclude unknown consequences. Physics-based probabilistic methods should eliminate safety factors as sources of unqualified uncertainty.
Obsolescence Management	The developer has analyzed and fully understands the developer's supply chain. The developer understands the reliability risks and design/manufacturing practices of the component and subassembly suppliers. The developer has also analyzed the potential for obsolescence of parts.
Parts, Materials and Processes Management	The developer incorporates parts, materials, and processes management in the overall Systems Engineering approach to assure proper application of parts, materials, and processes corresponding to the product life cycle stresses and reliability requirements.
Physics-based Probabilistic Analysis	Probabilistic analysis is used throughout the product life cycle beginning in the conceptual design phase in order to determine the criticality and sensitivity of various product subsystems/components to the product reliability and life-cycle cost, thereby focusing product design, modeling and simulation, and test and evaluation.
Quality Control	The developer has quality control procedures in place to make sure that the full reliability potential of the product design is maintained. The developer understands the manufacturing material and assembly variability and how they affect the product reliability.
Reliability Assessments prior to Formal Product-Level Test	Prior to entering a formal product-level test, the developer should have an engineering-based reliability assessment (based on the results of various reliability analyses, HALT, and other engineering tests) to show that there is a high probability of passing the test.
Reliability Improvement	The developer has a high-level and continuous focus on reliability improvement. The product design team is fully aware of the importance of high reliability and reliability is given a high priority.
Reliability Innovation	The developer has a history of applying innovative approaches to reliability (e.g., simplifying designs and improving manufacturing processes).
Reliability Past Performance	The developer's product design team has a history of producing reliable hardware and software.
Reliability Predictions	The developer does not rely solely on handbook predictions as an indicator of design status and maturity. Reliability predictions, based on handbooks or similar approaches, can be inaccurate and can lead to poor design decisions because the data used to develop the models for the predictions may not reflect current technology and/or current test and failure data. Developers and organizations in their supply chain that quote predictions may not understand the engineering and design considerations (such as operating temperatures and vibration environments) necessary to minimize risk and to produce a reliable design.
Reliability Program	The developer has a reliability program plan that is based upon realistic timelines, testing, and product design activities that will produce a product that meets the reliability requirements. Realistic delays associated with incorporating corrective actions should be identified and incorporated into the plan.
Reliability Staff	The developer has a sufficiently-sized reliability staff that is directly tied to the product design team.
Reliability vs. Cost	The developer does not equate increases in reliability with huge increases in cost. In many cases, significant improvements in reliability can be achieved at minimal cost, especially when reliability improvement is addressed as part of the product's design process.

Best Practice	**Description**
	Developers that see reliability increasing only through test-fix-test-fix-test process will likely not produce a cost-effective and reliable product.
Thermal and Vibration Analyses	The developer routinely conducts thermal and vibration analyses to address potential failure mechanisms and failure sites (i.e., a physics-of-failure approach to reliable product design). These analyses would likely include the use of fatigue analysis tools, finite element modeling dynamic simulation, heat transfer analyses, etc. Overall, the developer should have an integrated approach to design out many failures in the development process.

Annex C – Key Documents Matrix (Informative)

Annex A, Methods Matrix, provides references for the detailed "how to" for the various reliability tasks. This Annex shows the relationship of some of the key documents (plans and analysis) that span the Objectives of this standard. Some documents are direct outputs of the Objectives in this standard, and others are created outside of the reliability discipline but are used by reliability to communicate requirements to supporting organizations and subcontractors.

Document		Objective 1	Objective 2	Objective 3	Objective 4
		Understand Customer's Requirements	**Design and Redesign for Reliability**	**Production Reliability**	**Field Reliability**
		This is the core document from which the reliability requirements are flowed down.			
Reliability Program Plan (RPP)	System Requirements Review	Decompose/develop the customer's reliability requirements and allocate to each development and Integrated Product Team.	Update RPP based on design changes	Update RPP based on verification results	Update RPP based on analysis of delivered product
		Demonstrate the developers understanding of the customer's reliability requirements	Update RPP based on design changes	Update RPP based on verification results	Update RPP based on analysis of delivered product
	Reliability Allocations	Flow down the initial reliability requirements to the specifications and subcontractor statements of work.	Update Reliability Allocations based on design changes		
Parts Management Plan (PMP)		Provides parts selection criteria for the design, Integrated Product Teams and subcontractors.	Update PMP based on design changes	Update PMP based on potential obsolescence issues	Update PMP based on potential obsolescence issues
Reliability Case		Provide the current assessment of the Reliability Program	Update Reliability assessment of the Program	Update Reliability assessment of the Program	Update Reliability assessment of the Program
Performance Specifications		Flow down initial Reliability requirements to the specifications	Flow down finalized Reliability requirements to the specifications	Update specifications based on verification results	
Subcontractor Statement of Work		Flow down initial Reliability requirements to the subcontractor statement of work	Flow down finalized Reliability requirements to the subcontractor statement of work	Update subcontractor statement of work based on verification results	
Quality Control Plan			Flow down design and development quality requirements to design teams, Integrated Product Teams, and subcontractors	Flow down quality requirements for initial production	Flow down quality requirements for production and maintenance repairs
Closed-Loop Failure-Mode Mitigation Process (FRACAS)			Initiate, collect, and analyze data and make product changes	Collect and analyze data and make product changes	Collect and analyze data and make product changes
Design Verification Test			Conduct prototype and evaluation tests	Conduct design reliability growth, demonstration and qualification tests	
Warranty Analysis of Delivered			Establish warranty	Update warranty	Collect and analyze

Product		policy and procedures for returned product	policy and procedures	warranty data for returned product and make product changes

Annex D – Known Failure Definition and Scoring Criteria (Normative)

Government programs have reliability and maintainability failure description scoring criteria as part of the program's formal reliability assessment. The criterion is dependent upon the customer and can be a different from customer to customer. The customer and developer should jointly develop and agree on the definition and scoring of failures prior to the start of the formal reliability assessment.

Army-Specific

The US Army has specialized procedures exist for defining and scoring failures. A document termed the Failure Definition and Scoring Criteria (FDSC) is prepared for each system as required by Army Regulation 70-1, Army Acquisition Policy. The FDSC contains system-specific failure definitions as well as criteria for classifying and scoring failures. When the US Army is the customer, the Army FDSC ***shall*** be used to define and score failures.

Annex E – Acronyms (Informative)

The following list includes the list of acronyms used in this standard.

Acronym	Definition
ACIM	Availability Centered Inventory Model
ALT	Accelerated Life Test
BIT	Built-In Test
BOM	Bill of Material
CBM	Condition Based Maintenance
CFI	Customer Furnished Items
CIL	Configuration Item List
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMMI	Capability Maturity Model Integration
COTS	Commercial-Off-The-Shelf
DCACAS	Data Collection, Analysis and Corrective Action System
DMSMS	Diminishing Manufacturing Sources and Material Shortages
DoD	Department of Defense
DR	Deficiency Reporting
ECP	Engineering Change Process
EIA	Electronics Industry Association
ESS	Environmental Stress Screening
FDSC	Failure Definition Scoring Criteria
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Modes Effects and Criticality Analysis
FRACAS	Failure Reporting Analysis and Corrective Action System
GEIA	Government Electronic Industries Alliance
GEIA-STD	Government Electronic Industries Alliance Standard
GIDEP	Government Industry Data Exchange Program
HALT	Highly Accelerated Life Test
HASS	Highly Accelerated Stress Screen
ICOTE	Industrial Committee on Operational Test and Evaluation
IEC	International Electrotechnical Commission
IEEE	Industrial Electrical and Electronics Engineers
ISO	International Standards Organization
MDT	Maintainability Demonstration Test
MIL-STD	Military Standard
MTBF	Mean Time Between Failure
NATO	North Atlantic Treaty Organization
NDI	Non-Developmental Item
PCA	Physical Configuration Audit
PFMEA	Process Failure Modes and Effects Analysis
PFMECA	Process Failure Modes Effects and Criticality Analysis
PREDICT	Data Management Technique

Acronym	Definition
PRR	Production Readiness Review
QFD	Quality Function Deployment
RAM	Reliability, Availability and Maintainability
RCM	Reliability Centered Maintenance
RDGT	Reliability Development Growth Test
RIAC	Reliability Information Analysis Center
RPP	Reliability Program Plan
RQT	Reliability Qualification Test
SAE	Society of Automotive Engineers
SME	Subject Matter Experts
SOW	Statement of Work
SPC	Statistical Process Control
SVR	System Verification Review
TAFT	Test, Analyze, Fix, Test
TIGER	Simulation tool to forecast supply support requirements
TLCC	Total Life Cycle Cost
TOC	Total Ownership Cost
TQM	Total Quality Management
US	United States

ITAA Document Improvement Proposal

If, in the review or use of this document, a potential change is made evident for safety, health, or technical reasons please fill in the appropriate information below and mail or FAX to:

Information Technology Association of America (ITAA)
Standards & Technology Department
1401 Wilson Boulevard, Suite 1100.
Arlington, VA 22209
FAX: (703) 525-2279

Document No.	Document Title:
Submitter's Name:	Telephone No.: FAX No.: E-mail:
Address:	
Urgency of Change: _ Immediate:	_ At next revision:
Problem Area: a. Clause Number and/or Drawing: b. Recommended Changes: c. Reason/Rationale for Recommendation:	
Additional Remarks:	
Signature:	Date:
FOR ITAA USE ONLY Responsible Committee: Chairman: Date comments forwarded to Committee Chairman:	

ITAA

GEIA Group