ECSS–Q–00A
19 April 1996

Space Product Assurance

Policy and Principles

ECSS Secretariat
ESA–ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Published by: ESA Publications Division,
ESTEC, P.O. Box 299,
2200AG Noordwijk,
The Netherlands.

Price: 35 Dutch Guilders

Printed in the Netherlands

Foreword

This standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, National Space Agencies and European industry associations for the purpose of developing and maintaining common standards.

Requirements in this standard are defined in terms of what must be accomplished, rather than in terms of how to organise and perform the necessary work. This allows existing organisational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

The formulation of this standard takes into account the existing ISO 9000 family of documents.

This standard has been prepared by the ECSS Product Assurance Working Group, reviewed by the ECSS Technical Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Contents List

1

General

1.1 Scope

This Standard defines the Product Assurance (PA) policy, objectives, principles and rules for the establishment and implementation of PA programmes for projects covering mission definition, design, development, production and operations of space products including disposal.

The PA discipline covers: PA management, Quality Assurance, Safety Assurance, Reliability, Availability and Maintainability Assurance, Software Product Assurance, EEE Components, Materials, Mechanical Parts and Processes. It defines their respective objectives, policies, requirements and implementation standards to achieve the stated overall PA objectives throughout the complete life cycle of the products.

The provisions of this standard apply to space products. The requirements of this standard and its associated level 2 and 3 standards should be tailored to the needs and classes of specific projects.

1.2 Objectives

- The prime objective of Product Assurance is to assure that the Space Products accomplish their defined mission objectives and more specifically that they are Safe, Available and Reliable.
- A further objective is to achieve more cost–effective Space Projects and thereby to promote the competitiveness of the European Space Industry by coordinating the development and implementation of appropriate PA methods and standards.
- In support of project Risk Management, PA will assure an adequate identification, appraisal, prevention and control of technical risks within project constraints.

1.3 Policy

In order to meet these objectives, the ECSS PA policy is defined in this document. This policy requires a PA programme derived from a system based and preventive approach and includes:

- protection of human life, space products and services, investment and environment,
- definition and maintenance of a project PA function, with appropriate autonomy with respect to other lines and project level organisations,

- integrated application of the PA disciplines and coordination with the associated functions of project management and project engineering,
- tailoring of the PA requirements to the Project classes as defined in the ECSS Management standards,
- assignment of PA requirements and their control commensurate with the function criticality within the system,
- integrated PA participation to the overall risk management process,
- PA contribution to proper control of the technical risks and assuring awareness by the appropriate levels of management until the end of the disposal phase,
- implementation of a preventive approach, i.e. early identification of potential problems and continuous influence on the development process,
- verification activities consistent with project objectives,
- certification activities on the end product for customer's final acceptance.

1.4 PA Documentation Architecture

The ECSS Documentation Architecture, defined in the ECSS Standardization Policy document, identifies three levels.

The specific Levels 1 and 2 ECSS Product Assurance Standards are as follows:

Level 1:	ECSS–Q–00 =	Space Product Assurance – Policy and Principles
Level 2:	ECSS–Q–20 =	Space Product Assurance – Quality Assurance
	ECSS–Q–30 =	Space Product Assurance – Dependability
	ECSS–Q–40 =	Space Product Assurance – Safety
	ECSS–Q–60 =	Space Product Assurance – EEE Components
	ECSS–Q–70 =	Space Product Assurance – Materials, Mechanical Parts and Processes
	ECSS–Q–80 =	Space Product Assurance – Software Product Assurance

Level 3 standards, supporting implementation aspects of the above level 2 standards, will be defined whenever necessary.

2

Definitions and Abbreviations

2.1 Definitions

For the purposes of this standard, the definitions given in ECSS–P–001 Issue 1 apply.

2.2 Abbreviations

The following abbreviations are defined and used within this standard.

Abbreviation	Meaning
ECSS:	European Cooperation for Space Standardization
EEE:	Electrical, Electronic, Electromechanical
PA:	Product Assurance

(This page is intentionally left blank)

3

Product Assurance Management

3.1 Objective

The objective of Product Assurance Management is to ensure and achieve an adequate, effective and efficient coordination and implementation of the PA activities through a proper integration of the PA discipline as well as the integration of PA with all management and engineering activities.

3.2 Policy and Principles

The ECSS PA Management policy is that a PA programme is implemented throughout all project phases and coordinated with all the actors, and is managed in such a way as to:

- ensure that Project and PA organisation, requirements, methods, tools and resources are well defined before development and implemented at each level from system down to piece part,
- ensure that the applicable ECSS standards are tailored appropriately,
- ensure that aspects are identified, which could affect project requirements having major impacts on safety, mission success and the related cost and schedule consequences,
- ensure that adverse consequences of these aspects are prevented by the early detection, characterisation, elimination, minimisation and containment of problem contributors and initiators,
- ensure that risks are assessed and controlled, and that acceptability of the residual ones is evaluated,
- provide at any time the necessary visibility of the quality status of the product,
- ensure that the end product conforms to its specifications and that observed nonconformances are properly dispositioned.

The basic implementation principles are to:

- define, in a Product Assurance Plan all PA activities consistent with the Project objectives, requirements, criticalities and constraints,
- ensure the allocation and availability of adequate resources, personnel and facilities to carry out the required PA tasks,

- ensure that lower level contractors / suppliers perform proper PA monitoring and control,
- ensure proper progress monitoring, reporting and visibility of all PA matters, in particular those related to alerts, critical items, non-conformances, changes, deviations, waivers, actions and/or recommendations resulting from reviews, inspection and audits, qualification, verification and acceptance.

3.3 Requirements

3.3.1 Responsibility and Authority

a. The responsibility, the authority and the interrelation of personnel who manage, perform and verify work affecting quality shall be defined and documented.

b. The responsibilities and the interfaces of each organisation, either external or internal, involved in a project shall be defined and documented.

c. The delegation of product assurance tasks by a supplier to another lower tier supplier shall be done in a documented and controlled way. The supplier retains the responsibility towards the customer.

3.3.2 Resources

a. The supplier shall identify PA resource requirements.

b. The supplier shall provide adequate resources to perform the required PA tasks.

c. Trained personnel shall be assigned to the various PA activities.

d. The supplier shall establish a documented training programme for all personnel whose performance determines or affects product quality.

e. Reviews and audits of the product assurance programme, of processes and/or of product shall be carried out by personnel not directly involved in the work being performed.

3.3.3 Product Assurance Programme Management

a. The supplier shall assign a Project PA Manager from the PA line organisation, if any, reporting functionally to the Project Manager and having unimpeded access to higher management.

b. The appointed Project PA Manager, irrespective of other responsibilities, shall have sufficient organisational authority and independence:

   1. to propose and maintain a product assurance programme in accordance with the project product assurance requirements.
   2. to have unimpeded access to higher management through the company PA (or equivalent) executive as necessary to fulfil his duties.

c. The supplier shall prepare and implement a project product assurance plan to be approved by the customer.

d. The supplier's product assurance plan shall be maintained throughout the project life cycle.

   The product assurance plan may refer to clauses of the Company Quality Manual and to in-house procedures.

e. The supplier shall report on a regular basis as specified in the business agreement on the status of the product assurance programme implementation.

f. The supplier shall plan and perform quality audits using established and maintained procedures.

3.3.4 Contractual Aspects

a. All contracts shall include suitable product assurance provisions based upon the knowledge of the products and on purchaser's requirements.

b. The product assurance function shall be involved in the preparation and negotiations of the product assurance provisions.

c. The product assurance function shall participate in the detailed review of the contract.

d. The product assurance function shall be involved in the assessment and review of all changes to the contractual requirements.

3.3.5 Risk Assessment and Control

a. The supplier shall perform a systematic risk assessment, reduction and control of risks in achievement of required technical performance, within the project cost and schedule constraints.

b. The risk assessment, reduction and control Process shall include inputs from all Product Assurance disciplines and shall contribute to the overall project risk management process required in ECSS–M–00.

c. Risk Identification

In identification of risk, the following aspects shall be systematically considered:

- Difficulties or uncertainties expected in demonstration of design performance, and with items having poor design margins.
- Risk identified by Dependability and Safety analyses.
- Difficulties or uncertainties expected in development of new products, components, parts, materials and processes.
- Difficulties or uncertainties expected in procurement, manufacturing, assembly, inspection, test, handling, storage and transportation, which may lead to unacceptable degradations in the quality of the product.
- Difficulties anticipated in product utilisation or service implementation.
- Risk identified by suppliers at lower levels.
- Risk of product quality degradation as the result of cost and schedule constraints imposed on the project.

d. Critical Item

Critical items shall be identified as a result from risk assessment. The project shall define the criteria for critical item identification, taken into account the capability for detection and control of risk occurrence.

e. Dependability and Safety

1. The Dependability and Safety concept of technical risk identification, reduction and control is part of the project "Risk Management Process", which shall be a continuous and iterative process throughout the project life cycle.

   The Dependability and Safety related technical risk reduction and control process are joint activities of the Dependability and Safety and respective engineering domains. The process of risk identification will be performed by applying simultaneously two approach principles:

   * Top-Down Approach

     In the top-down approach, Dependability and Safety Engineering start with analysis – based principally on past experience – and the given Dependability and Safety objectives. On the basis of the system feared

events (e.g. loss of life, loss of mission, etc.), an event tree is constructed (e.g. by using a Fault Tree Analysis – FTA) to identify the worst case events/failures at the boundaries between system, subsystem and equipment.

* Bottom-Up Approach

  In the bottom-up approach, Dependability and Safety Engineering start with a detailed analyses undertaken on product (e.g. by using a Failure Mode Effect and Criticality Analysis – FMECA). All failure modes are assessed for risk potential and event consequences are followed up to the next level of integration up to system level. Risk reduction actions are taken at the best suitable level. Where outlines of failure cases are defined, corresponding system studies are feasible.

2. The Dependability and Safety related technical risk reduction and control process shall be applied to all identified hazards and failure modes, which have unacceptable consequences at any time in the project.
3. In identification of failure modes and hazards and associated technical risks duly consideration shall be given on past experience, studies, ground and flight tests, reviews, the industrial process as well as the operational use.
4. The process of risk identification and assessment employs both qualitative and quantitative approaches.
5. All identified technical risks have to be assessed primarily for their consequence severity and categorized according to the appropriated project severity category and corresponding controls shall be recommended.
6. Dependability and Safety activities shall be co-ordinated.
7. After qualitative risk reduction is applied, the residual risks including probability shall be evaluated. The acceptability of these residual risks shall be justified according to defined criteria.
8. Risk reduction measures as proposed for Dependability and Safety shall be assessed at system level in order to select the optimum solution to reduce the system level risk.

4

Quality Assurance

4.1 Objective

The objective of Quality Assurance is to provide adequate confidence to the customer that the end product or service satisfies the requirements.

4.2 Policy and Principles

The ECSS Quality Assurance policy is to ensure, in conjunction with other integrated project and PA functions, that required quality is specified, designed-in and will be incorporated, verified and maintained in the relevant hardware, software and associated documentation throughout all project phases, by applying a programme where:

- assurance is provided that all requirements are adequately specified,
- design rules and methods are consistent with the project requirements,
- each applicable requirement is verified through a verification programme which includes one or more of the following methods: analysis, inspection, test, review of design, audits,
- design and performance requirements including the specified margin are demonstrated through a qualification process,
- assurance is provided that the design is producable and repeatable, and that the specification of the resulting product can be verified and operated within the required operating limits,
- adequate controls are established for the procurement of components, materials, software and hardware items, services,
- fabrication, integration, test and maintenance are conducted in a controlled manner such that the end item conforms to the applicable baseline,
- a nonconformance control system is established and maintained in order to track nonconformances systematically and to prevent reoccurrence,
- quality records are maintained and analysed to report and detect trends in due time for preventive / corrective actions,
- inspection, measuring and test equipment and tools in use on the contract are controlled to be accurate for their application,
- procedures and instructions are established which provide for the identification, segregation, handling, packaging, preservation, storage and transportation of all items,
- assurance that the operations including post-flight and disposal are carried out in a controlled way and in accordance with the relevant requirements.

4.3 Requirements

The detailed Quality Assurance requirements are defined in ECSS–Q–20, in accordance with the above policy and principles.

5

Safety Assurance

5.1 Objective

The objective of Safety Assurance is to ensure that all safety risks associated with the design, development, production and operations of Space Product are adequately identified, assessed, minimised, controlled and finally accepted through the implementation of a safety assurance programme.

5.2 Policy and Principles

The ECSS Safety policy is:

- to ensure that space systems will not cause a hazard to, in order of priority:
  - human life,
  - the environment,
  - public and private property,
  - spacecraft and launcher,
  - ground support equipment and facilities,
- to determine and evaluate the safety risks associated with Project activities,
- to minimise safety risks in a technically effective and cost effective manner,
- to ensure adequate verification of safety control measures.

The ECSS safety policy shall be implemented by applying a safety programme which shall ensure that:

- safety is designed into the system;
- safety controls are adequately implemented in the verification plan,
- safety requirements including launch centre safety regulations are met,
- hazards are identified, and eliminated or, where this is not possible, minimised, ranked and controlled in accordance with Project objectives in a manner acceptable to the customer and to the safety organisations involved in the implementation of the mission.

The Safety Programme shall comprise:

- the identification and control of all safety related risks with respect to the design, development and operations of space products,
- the assessment of the risks based on qualitative and quantitative analysis as appropriate,
- the application of a hazard reduction precedence and of control measures of the residual risks.

5.3 Requirements

The detailed Safety Assurance requirements are defined in ECSS–Q–40 in accordance with the above policy and principles.

6

Dependability Assurance

6.1 Objective

The objective of the Dependability Assurance is to ensure system availability to achieve a successful mission at minimum life cycle costs.

6.2 Policy and Principles

The ECSS dependability policy is to:

- identify all technical risks with respect to functional needs which can lead to noncompliance with dependability requirements,
- apply appropriate analysis and design methods to ensure that dependability targets are met,
- optimise the overall cost and schedule by making sure that:
  - design rules, dependability analyses and risk reducing actions are tailored with respect to an appropriate criticality categorisation,
  - risks reducing actions are implemented continuously since the early phase of a project and especially during the design phase,
- provide appropriate inputs to the Integrated Logistics Support activities.

6.3 Requirements

The detailed Dependability Assurance requirements are defined in ECSS–Q–30 in accordance with the above policy and principles.

(This page is intentionally left blank)

7

Software Product Assurance

7.1 Objective

The objective of the Software Product Assurance is to ensure that developed or reused software and software services satisfy the requirements. In particular, the software shall perform properly and safely in the operational environment.

7.2 Policy and Principles

The Software PA policy is directly derived from the general PA policy. It is implemented by applying a programme where:

- all software requirements are adequately specified,
- all software applications are categorised according to criticality,
- appropriate design and development methods and standards are established and applied in accordance with software categories,
- development and maintenance processes are continually monitored,
- any software problems are found and corrected with sufficient timeliness to minimise their impact,
- performance requirements are demonstrated through customer agreed qualification and acceptance tests,
- verification and validation are properly achieved,
- design, implementation and inspection allow a real capability to maintain and/or to reuse software.

7.3 Requirements

The detailed Software Product Assurance requirements are defined in ECSS–Q–80 in accordance with the above policy and principles.

(This page is intentionally left blank)

8

Electrical, Electronic, Electromechanical (EEE) Components

8.1 Objective

The objective associated to EEE components is to ensure that the components will satisfy the mission performance requirements during the full life cycle of the products.

8.2 Policy and Principles

The ECSS components policy in this area is:

- to select components which are capable of meeting the functional performance, lifetime, environmental, safety, quality and reliability requirements;
- to minimise risks by making sure that:
  - all critical technologies or applications are identified and controlled,
  - all components are identified, evaluated and controlled by a procurement specification,
  - all nonconformances are properly treated,
- to optimise the overall costs and schedules by making sure that:
  - the technical and programmatic requirements are tailored to the specific application with respect to an established quality level of the components,
  - a stringent component standardization programme is implemented to avoid duplication of efforts,
  - the procurement system is under control and includes proper monitoring and reporting,
  - all major activities including back-up solutions are planned and initiated in time to match project needs;
- to promote the usage of European components.

8.3 Requirements

The detailed EEE Component requirements are defined in ECSS–Q–60 in accordance with the above policy and principles.

(This page is intentionally left blank)

9

Materials, Mechanical Parts and Processes

9.1 Objective

The objective associated to Materials, Mechanical Parts and Processes is to ensure that their use will satisfy the mission performance requirements.

9.2 Policy and Principles

The ECSS policy in the area of materials, mechanical parts and processes is:

- to select rigorously those items which can fulfil the functional requirements during a lifetime compatible with mission duration and in the specific environmental conditions,
- to rely on available space proven technologies whenever possible,
- to identify and control all new products, critical materials, and mechanical parts and processes,
- to make the best use of all available research, including the technology programmes of European space agencies.

An efficient implementation programme shall be defined, covering the selection, characterisation, evaluation, qualification for their intended use and procurement of the materials, mechanical parts and processes.

This programme shall in particular identify and validate critical applications in due time for safe utilisation and lead to cost-effective solutions through a type reduction and standardization process.

9.3 Requirements

The detailed Materials, Mechanical Parts and Processes requirements are defined in ECSS–Q–70 in accordance with the above policy and principles.