ESA PSS-01-21 Issue 2
April 1991

Software product assurance requirements for ESA space systems

Prepared by:
Product Assurance and Safety Department and
ESA Fracture Control Board
European Space Research and Technology Centre
Noordwijk, The Netherlands

Approved by:
The Inspector General, ESA

european space agency / agence spatiale européenne
8-10, rue Mario-Nikis, 75738 PARIS CEDEX, France

Published by ESA Publications Division
ESTEC, Noordwijk, The Netherlands.

Printed in the Netherlands.

ESA Price code: E0

ISSN 0379 - 4059

ABSTRACT

This specification contains the product assurance requirements for the software developed for ESA space systems where other level 2 PSS-01 specifications are applicable. It supports the ESA Software Engineering Standard PSS-05-0 and explains the functions of product assurance, its management and the activities performed by product assurance for each phase of the software life-cycle.

DOCUMENT CHANGE RECORD

Issue number and date	Sections affected	Remarks
Issue 1 February 1983	All	New document
Issue 2 April 1991	All	Document completely revised.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

SECTION 1: INTRODUCTION

1.1 SCOPE

This standard defines the ESA Software Product Assurance (SPA) requirements to be implemented during the development and operation of software for space systems where other ESA PSS-01 level 2 documents have been made applicable. It supports ESA PSS-05-0, ESA Software Engineering Standards.

1.2 APPLICABILITY

These requirements shall apply whether the contract is for software alone or for software as a portion of a system. These requirements also apply to software developed as part of a subcontract or otherwise procured for use in individual programmes.

Product Assurance includes the disciplines of Reliability, Maintainability, Safety, Quality Assurance, and Configuration Management as defined in ESA PSS-01-0. The application of these disciplines to software is called Software Product Assurance (SPA).

Each of these disciplines is applied to a complete system under development. Where software is a part of the system, the assurance of the software shall be specifically addressed within the scope of these disciplines and not as a separate discipline. However, SPA activities and milestones are an integral part of the software development. They shall be identified in the Software Management Plan (SMP) and controlled according to the life cycle identified in ESA PSS-05-0.

1.3 APPLICABLE DOCUMENTS

The following ESA documents, of the issue specified in the contract, form part of this document to the extent specified herein:

PSS-01-0 Product Assurance and Safety Policy and Basic Requirements for ESA Space Systems
PSS-01-10 Product Assurance Management Requirements for ESA Space Systems
PSS-01-11 Configuration Management and Control for ESA Space Systems
PSS-01-20 Quality Assurance Requirements for ESA Space Systems
PSS-01-30 Reliability Requirements for ESA Space Systems
PSS-01-40 System Safety Requirements for ESA Space Systems

PSS-01-50 Maintainability Requirements for ESA Space Systems
PSS-05-0 ESA Software Engineering Standards

1.4 DEFINITIONS

The definitions of terms used in this document are contained in Appendix A.

1.5 ORGANISATION

Section 1 of this document identifies the scope, applicability and applicable documents for this standard. Section 2 identifies the functions and policies of Software Product Assurance with regard to the software development process. Section 3 identifies the overall management and control requirements on the Software Product Assurance process. Each subsequent section identifies the activity requirements for a particular phase of the software life cycle starting with the User Requirements Definition Phase and ending with the Operations and Maintenance Phase.

SECTION 2: SOFTWARE PRODUCT ASSURANCE FUNCTIONS

In support of the overall system Product Assurance effort, it is the function of SPA to:

a) Establish and maintain the Software Product Assurance Plan and assure that the Configuration Management Plan conforms to the requirements established for the programme;

b) Provide support to the production of the User Requirements Document (URD) defined in ESA PSS-05-0, to assure in particular that the software quality, reliability, safety, maintainability, and configuration management requirements are defined;

c) Participate in the assessment and review of the project-specific standards, methodologies and tools for software development, control, and verification against the approved requirements contained in the URD;

d) Establish and maintain the standards and methodologies for Software Product Assurance and Configuration Management; e)as part of the regular software development life cycle, assess and evaluate system safety, reliability and maintainability characteristics of the software against defined requirements;

f) Assure that the approved standards, methodologies and tools are applied throughout the software life cycle;

g) Implement a closed-loop reporting and tracking system for the identification and correction of nonconformances to requirements or procedures;

h) Systematically collect data associated with the methodologies used in the life cycle and the software products produced;

i) Assure that traceability is maintained through all phases of the software life cycle, and;

j) Assure that the Software Verification Plan (SVP) completelycovers all requirements and that the Software Verification Report (SVR) is correctly completed.

PAGE INTENTIONALLY LEFT BLANK

SECTION 3. SOFTWARE PRODUCT ASSURANCE MANAGEMENT

3.1 ORGANISATION AND RESOURCES

Software PA responsibilities shall be identified for each PA discipline consistent with the requirements of the PA standards identified in Table 3-1.

TABLE 3.1: ESA PRODUCT ASSURANCE STANDARDS

Configuration Management	PSS-01-11
Quality Assurance	PSS-01-20
Reliability	PSS-01-30
Safety	PSS-01-40
Maintainability	PSS-01-50

The Product Assurance Manager shall assure that the responsible groups are provided with the resources needed to perform the SPA tasks and verify the correct and timely performance of each task. He shall assure that the personnel performing the SPA tasks have been trained to perform those tasks, and that their performance is adequate to meet the contractual requirements. The Software PA activities shall be integrated into the software life cycle defined in ESA PSS-05-0.

3.2 PLANNING

The Product Assurance organisation shall prepare and maintain a Software Product Assurance Plan in accordance with Appendix B. An initial plan shall be produced at the start of the development programme. This plan shall be updated and reviewed at the end of each life-cycle phase. The minimum acceptance criteria for the plan at each review shall include definition of the SPA programme for the next life-cycle phase.

3.3 INFORMATION FLOW

3.3.1 Right of access

ESA, or an ESA representative, shall retain the right to audit any supplier of software. All information associated with the methodologies used in the life cycle and the software products being produced shall be made available for evaluation. This shall include access to individuals or facilities needed to obtain or verify the information.

3.3.2 Progress reporting

SPA shall attend all project software progress meetings. SPA shall assure that the agenda is in accordance with ESA PSS-05-0 and all items are discussed. SPA shall provide data and report on SPA activities under the appropriate agenda item. SPA shall also report to the overall PA function. Reporting and data presented shall include:

a) Number and status of nonconformances which includes;
   i) rate of detection;
   ii) nonconforming product components;
   iii) processes introducing nonconformances;
   iv) processes detecting nonconformances;
b) Adequacy of SPA activities;
c) Status of development facilities;
d) Status of training;
e) Adherence to standards;
f) Deviations from plans;
g) Potentially serious trends or deviations from trends;
h) Significant audit or inspection activities;
i) Aspects relating to the integration of SPA to the overall PA activities.

3.3.3 Nonconformance control

The Nonconformance control system defined in ESA PSS-01-20 shall be used for reporting, analysing, and tracking software nonconformances discovered in the software, associated documentation and activities. Nonconformances shall be identified to the lowest level of configuration item.

Nonconformance and configuration control shall start for code at the time of satisfactory acceptance of a software unit or module in a software system. For documentation, nonconformance control, reporting and configuration control shall start after the first review and approval of the document. The tracking and reporting system for nonconformances shall allow the evaluation of the impact of nonconformances so that priorities for the use of resources may be established.

3.4 SOFTWARE PRODUCT ASSURANCE PROCEDURES

The project specific standards shall include standards to meet the requirements of this document. These standards shall identify the procedures for control and monitoring the software development and shall include the following SPA requirements:

a) *Quality Audits* - procedures for ensuring that the approved methods and tools are correctly applied.
b) *Quality Control and Reporting* - procedures for the documentation and tracking of nonconformances during development.
c) *Reviews* - procedures for performing reviews.
d) *Verification and Validation* - procedures for the support provided by SPA in assuring that the SVP is produced according to the approved standards, Verification and Validation (V&V) is performed correctly, and an SVR is provided.
e) *Configuration Management* - procedures used to meet the configuration management requirements defined in ESA PSS-05-0 and ESA PSS-01-11.
f) *Classification* - procedures based on methods described in ESA PSS-01-30 and ESA PSS-01-40 to classify a software product
according to its functional criticality.
g) *Development Statistics* - procedures for the collection and analysis of development statistics.

For each procedure, the following shall be identified:
- the scope of the procedure;
- inputs required to initiate the procedure;
- resources required for implementation of the procedure;
- a step-by-step definition of the implementation of the procedure;
- the format and content of outputs and the recipient of each output;
- provisions for corrective action;
- methods for verifying correct completion.

3.5 SOFTWARE CLASSIFICATION

Software shall be classified according to its functional criticality using the Failure Effect Severity Categories and Hazard Consequence Severity Categories described in ESA PSS-01-30 and ESA PSS-01-40. SPA shall assure that the classification is performed using the correct methods and that the required implementation standards are enforced.

3.6 DEVELOPMENT STATISTICS

Development statistics shall be collected during the software life cycle. They shall be stored in a central location for analysis and use, and shall be delivered in the Project History Document (PHD). Data shall be collected to provide information about:

a) *requirement stability* - the rate of change requests attributed to change in requirements,
b) *design stability* - the rate of design change compared with the initial approved design;
c) *error profiles* - distribution of error introduction and error detection throughout the life cycle;
d) *test evaluation* - type and number of errors revealed per test case;
e) *productivity* - effort expended in the different life cycle phases;
f) *product information* - size, elapsed time to produce the product, size of support software required, cost of infrastructure etc.

3.7 SUBCONTRACTED AND PURCHASED SOFTWARE

The developing organisation shall assure that a subcontractor developing software adheres to the requirements in this document. All audit and review records shall be retained on file and be available for review by ESA during development and maintenance of the system.

For purchased and reused software, SPA shall:

a) assure that the data rights and documentation comply with contractual requirements;
b) assure that an SRD is produced which is traceable to the URD;
c) assure that the software verification is planned and performed against the SRD;
d) assure that the software is correctly classified and appropriate controls are applied as defined in Section 3.5.

SECTION 4. USER REQUIREMENTS PHASE ACTIVITIES

The remainder of this document describes Software Product Assurance activities in each phase of the software life cycle defined in ESA PSS-05-0.

4.1 REQUIREMENTS DEFINITION

Software ESA PA shall provide support to the production of the URD defined in ESA PSS-05-0 to assure in particular that the software safety, quality, reliability, maintainability, and configuration management requirements are defined and are consistent with the documents identified in Section 1.3 of this document. SPA shall assure that the experience gained from previous software projects is considered for incorporation into the URD and that the requirements for collecting development statistics are included.

4.2 TRACEABILITY

SPA shall assure that the requirements of the URD are traced to the appropriate system requirements and that these system requirements are traced to the URD requirements. SPA shall assure that this traceability is maintained in the event of changes to these documents according to ESA PSS-01-11.

4.3 PLANNING

The initial SPA Plan shall be written and submitted for approval to the Agency as defined in Section 3.2.

4.4 PHASE MONITORING ACTIVITIES

SPA shall monitor:
- the requirements definition process to ensure that the approved procedures for the generation and review of the URD are applied;
- the processes used to generate the SMP for conformance to approved procedures.

4.5 REVIEWS

SPA shall assure that:
- the URD conforms to the requirements identified in ESA PSS-05-0 Part 1 Chapter 2;
- each requirement has quantified parameters allowing verification to be performed;
- reviews are conducted according to approved procedures.

SPA shall participate in all formal reviews of software documents and processes.

PAGE INTENTIONALLY LEFT BLANK

SECTION 5: SOFTWARE REQUIREMENTS PHASE ACTIVITIES

5.1 TRACEABILITY

SPA shall assure that traceability is documented and maintained in both directions between the URD and:
- the SRD
- the SMP
- the SPA Plan
- the CM Plan.

SPA shall assure traceability and baseline definition between the procedures defined in the Software Test Plan (STP) and the requirements in the SRD to be verified by test according to ESA PSS-01-11.

5.2 PLANNING

The SPA Plan shall be updated as defined in Section 3.2 to identify the organisation, activities, procedures, and schedule for SPA in the Architectural Design Phase. This shall include the definition of all Mandatory Inspection Points (MIP) and Key Inspection Points (KIP) as defined in ESA PSS-01-20, and the planning for the collection and use of software metrics.

A MIP/KIP is a review activity in which the Agency requires participation. This includes activities such as software audits, walkthroughs, inspections, reviews of static/dynamic analyses or others as determined by the Agency's PA Manager.

SPA shall provide inputs to the verification and qualification plans. This shall include definition of the SPA activities, standards, and tools in those processes.

5.3 PHASE MONITORING ACTIVITIES

SPA shall monitor the:
- requirement-definition process to ensure that the approved procedures for the generation and review of the SRD are applied;
- processes used to update the SMP for conformance to approved procedures;
- processes used to produce the CM Plan, the SPA Plan and the SVP.

SPA shall assure that:
- regular progress meetings take place with an approved agenda;
- any URD requirement which is not satisfied is identified by an NCR.

SPA shall attend the progress meetings.
SPA shall conduct the following analyses to identify safety and reliability nonconformances:
- Failure Mode Effects and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA) as defined in ESA PSS-01-30.
- Hazard Analyses identified in ESA PSS-01-40.
- Risk Assessment identified in ESA PSS-01-40.

5.4 REVIEWS

SPA shall assure that:
- the SRD conforms to the requirements of ESA PSS-05-0;
- each requirement has quantified parameters allowing verification to be performed;
- the updated SMP conforms to ESA PSS-05-0;
- CM Plan conforms to the requirements of ESA PSS-05-0 and ESA PSS-01-11;
- SPA Plan conforms to the requirements of this document;
- reviews are conducted according to approved procedures.

SPA shall participate in all formal reviews of software documentation.

5.5 DATA COLLECTION

SPA shall assure that the appropriate development statistics as detailed in the SMP are collected and stored. (ref. Section 3.6)

SECTION 6: ARCHITECTURAL DESIGN PHASE ACTIVITIES

6.1 TRACEABILITY

SPA shall assure that traceability is documented and maintained in both directions between the SRD requirements and:
- ADD design elements
- STP procedures.

6.2 PLANNING

SPA shall support the update of:
- the SPA Plan
- the CM Plan.

6.3 PHASE MONITORING ACTIVITIES

SPA shall monitor:
- the architectural design definition process to ensure that the approved methodologies and tools are used for the generation of the ADD;
- that the processes used to update the SMP, CM Plan, SPA Plan, and SVP conform to approved procedures;
- the updating of the STP to ensure comprehensive testing;
- adherence to procedures defined in the SMP, CM Plan, and SPA Plan.

SPA shall assure that:
- regular progress meetings take place with an approved agenda. SPA shall attend the progress meetings;
- the software developers are aware of any changes to requirements in the URD and SRD;
- any requirement which is not satisfied at the architectural design level is identified by an NCR;
- a project coding standard is available.

The analyses identified in Section 5.3 shall be updated according to information produced in the Architectural Design Phase.

6.4 REVIEWS

SPA shall assure that the:
- ADD conforms to the requirements of ESA PSS-05-0 Part 1 Chapter 4.;
- STP conforms to the requirements identified in ESA PSS-05-0 Part 2 Chapter 4. SPA shall assure that the classification of the software has been properly considered in the proposed tests;
- updated SMP conforms to ESA PSS-05-0;

- SVP has been completed and all requirements are appropriately referenced;
- updated CM Plan conforms to the requirements of ESA PSS-05-0 and ESA PSS-01-11;
- updated SPA Plan conforms to the requirements of ESA PSS-05-0 or this document, as required;
- reviews are conducted according to approved procedures.

SPA shall participate in all formal reviews of software documentation.

6.5 DATA COLLECTION

SPA shall assure that the appropriate development statistics as detailed in the SMP are collected and stored. (ref. Section 3.6).

SECTION 7: DETAILED DESIGN PHASE ACTIVITIES

7.1 TRACEABILITY

SPA shall assure traceability is documented and maintained in both directions between:
- ADD design elements and the detailed design modules;
- the DDD modules and the STP procedures.

7.2 PLANNING

The SPA Plan shall be updated to identify the relevant SPA activities, procedures, and schedule for the Transfer Phase. This shall include defining the activities required to support the installation and checkout of the software or system.

7.3 PHASE MONITORING ACTIVITIES

SPA shall monitor:
- the detailed design definition process to ensure that the approved methodologies and tools are applied;
- the coding process to ensure that the approved methodologies, standards and tools are applied;
- adherence to the procedures identified in the SMP, CM Plan, SPA Plan and STP;

SPA shall assure that:
- regular progress meetings take place with an approved agenda. SPA shall attend the progress meetings;
- the CM process functions to inform software developers of any changes to requirements in the URD, SRD or design documents;
- any requirement which is not satisfied at the detailed design level is identified by an NCR.

The analyses identified in Section 5.3 shall be updated according to information produced in the Architectural Design Phase.

7.4 REVIEWS

SPA shall assure that the:
- DDD conforms to the requirements of ESA PSS-05-0 Part 1 Chapter 4;
- code listings conform to the project coding standard;
- Software User Manual (SUM) conforms to the requirements of ESA PSS-05-0 Part 1 Chapter 5;
- STP conforms to the requirements of ESA PSS-05-0 Part 2 Chapter 4;
- reviews are conducted according to approved procedures.

SPA shall participate in all formal reviews of the software.

7.5 DATA COLLECTION

SPA shall assure that the appropriate development statistics as detailed in the SMP are collected and stored. (ref. Section 3.6)

SECTION 8: TRANSFER PHASE ACTIVITIES

8.1 TRACEABILITY

SPA shall assure that the traceability records for all documentation are kept current with the project baselines as changes are made to the system. SPA shall assure that the as-verified configuration status of the software is identified and maintained as defined in ESA PSS-01-11, and that it is traceable to the detailed design.

8.2 PHASE MONITORING ACTIVITIES

SPA shall monitor:
- acceptance testing to ensure that it is in accordance with the STP;
- adherence to the procedures identified in the SMP, SPA Plan and CM Plan;

SPA shall assure that:
- the software submitted for acceptance is the latest correctly configured version;
- all acceptance test activities are correctly documented;
- all deliverable code and documentation are correctly recorded in the Configuration Management system;
- a Project History Document (PHD) is produced in accordance with ESA PSS-05-0.

The analyses identified in Section 5.3 shall be updated according to the changes and information produced during the Transfer Phase.

8.3 REVIEWS

SPA shall assure that:
- the Software Transfer Document complies with the requirements of ESA PSS-05-0;
- reviews are conducted according to approved procedures.

In addition to assuring the test documentation, SPA or its delegate, shall witness all acceptance tests, certify the activities and results, and assure the integrity of the test article, test data, and reporting of problems and results.

8.4 VERIFICATION

SPA shall support the verification of software by producing the Software Verification Report (SVR). The SVR shall record the verification of requirements and provide cross references to the particular processes involved in the verification. SPA shall assure that all requirements are verified.

SPA shall assure that all nonconformances have been resolved prior to the completion of the Transfer Phase.

8.5 DATA COLLECTION

SPA shall assure that the appropriate development statistics as detailed in the SMP are collected and stored. (ref. Section 3.6)

SECTION 9: OPERATIONS AND MAINTENANCE PHASE ACTIVITIES

9.1 TRACEABILITY

SPA shall assure that the traceability records for all documentation are updated and kept current with the project baselines as changes are made to the system. SPA shall assure that the as-verified configuration status of the software is identified and maintained as defined in ESA PSS-01-11, and that it is traceable to the detailed design.

9.2 CONFIGURATION MANAGEMENT

SPA shall assure that all deliverables from the developer are controlled by the Configuration Management system, and that all modifications are properly processed under this system as defined in the approved CM Plan. SPA shall assure that all software and documentation delivered by the developer are available during the Operations and Maintenance Phase.

9.3 PHASE MONITORING ACTIVITIES

SPA shall assure that all agreed modifications are incorporated into the documentation and that the appropriate tests and verification activities are performed to ensure satisfactory implementation of the modifications.

9.4 DATA COLLECTION

SPA shall assure that the appropriate development statistics as detailed in the SMP are collected and stored. (ref. Section 3.6).

PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

DEFINITIONS OF TERMS

This appendix will be superseded by ESA PSS-01-001 when that document is approved by the Agency.

The terminology used in this standard is in general in accordance with the 'IEEE Standard Glossary of Software Engineering Terminology', IEEE Standard 729-1983. This Appendix is a list of terms which are not contained in the IEEE document.

CRITICAL SOFTWARE

A defined set of software components which have been evaluated and whose continuous correct operation has been determined to be essential for safe and reliable operation of the system. Critical software is composed of two independent elements: Reliability Critical Software and Safety Critical Software

DEFECT

A mistake in the design or instantiation of the system. This will under appropriate initiating conditions result in a fault in system operation. A Defect causes a Fault which may result in a Failure.

DEVELOPMENT

All activities performed to transform a set of user requirements into an end product ready for use. This includes requirements definition, design, manufacture, qualification, integration, validation and verification.

HARDWARE/SOFTWARE INTERFACE

The specified boundary between hardware and the software that controls its operation.

INSTALLATION

1. A single hardware machine capable of running one or more instances of a software product.
2. The process of integrating the system into its operational environment and verifying that it performs as required.

NONCONFORMANCE

1. A deviation from the actual or intended definition of an item.
2. Incorrect or incomplete implementation of specific requirements at a lower level of design.

OPERATIONAL PROFILE

A definition of the conditions of use for a system. Input values to the system are defined in terms of their distribution by time or probability from the range of possible inputs.

RELIABILITY CRITICAL SOFTWARE

Software which has been evaluated and found to have a Functional Effect Severity Category (see ESA PSS-01-30) of 1 or 2.

SAFETY CRITICAL SOFTWARE

Software which has been evaluated and found to:
a) have a Hazard Consequence Category (see ESA PSS-01-40) of I; or
b) perform Emergency Caution and Warning functions; or
c) initiate Escape and Rescue functions.

SOFTWARE

Computer programmes, procedures, rules, and associated documentation and data pertaining to the operation of a computer system.

UNIT

1. The smallest logical entity specified in the detailed design which completely describes a single operation independent of any other operations. A module is composed of one or more units.
2. The code for a single cohesive operation written from the detailed design and tested independently of other units.

WORK PROCESS

An activity performed to produce items required for the definition, design, development, assessment or maintenance of a system.

WORK PRODUCTS

The outputs of work processes. Work products may be documents such as requirement specifications, design specifications, procedures and manuals, or may be elements of the delivered system such as code, components, assemblies and configuration items.

APPENDIX B

SOFTWARE PRODUCT ASSURANCE PLAN

DATA ITEM DESCRIPTION (DID)

PAGE INTENTIONALLY LEFT BLANK

SOFTWARE PRODUCT ASSURANCE PLAN

Preparation Instructions

1.0 INTRODUCTION

This paragraph shall identify the scope, purpose and contents of this document.

1.1 IDENTIFICATION

This paragraph shall contain the following: The Software Product Assurance Plan defines the implementation of the Product Assurance policies on the [insert programme name] programme. These policies are implemented to meet the requirements of ESA PSS-01-21, ESA Software Product Assurance Requirements, and of [insert programme requirements document identity], [insert programme requirements document title]. This document is identified as [insert configuration item name] Software Product Assurance Plan and is written in compliance with Appendix B of ESA PSS-01-21.

1.2 SCOPE

This paragraph shall identify the scope of application of the contents of this document with regard to the system being developed. It shall identify all restrictions in application and interfaces with other plans.

1.3 PURPOSE

This paragraph shall briefly identify the purpose of the system and identify the elements of the configuration item(s) to which the plan applies.

1.4 ORGANISATION

This paragraph shall describe the organisation of the Software Product Assurance (SPA) Plan.

1.5 SYSTEM DESCRIPTION

This optional paragraph may be used to describe the configuration and operation of the system or portion of the system to which the SPA Plan applies.

2.0 DOCUMENTS

This Section shall identify the specific issue of all documents used in the generation of the SPA Plan. This Section shall contain the following paragraphs:

2.1 APPLICABLE DOCUMENTS

This paragraph shall identify all (but only) documents specifically referenced in the text of the SPA Plan. This paragraph shall begin with the following sentence:
"The following documents, of the exact issue shown, form a part of this document to the extent specified herein."

Applicable documents shall be listed by document number, version or revision identification, and full title in the following order:
1.Specifications
2.Standards
3.Drawings
4.Other publications

Copies of specifications, standards, drawings, and publications required by suppliers in connection with specified procurement functions are to be obtained from the procuring activity or as directed by the contracting officer.

2.2 INFORMATION DOCUMENTS

This paragraph shall begin with the following sentence:
"The following documents, although not a part of this document, amplify or clarify its contents."

Information documents shall be listed by document number, source and full title in the following order:
1.Specifications
2.Standards
3.Drawings
4.Other publications

2.3 PARENT DOCUMENTS

This paragraph shall identify the requirements document and any higher-tier plans which establish the technical basis for this document by document number, version or revision identifier and full title.

3.0 MANAGEMENT

This section shall describe the organisation, structure and responsibilities for Software Product Assurance for all phases of the life-cycle. This shall include those activities required to assure the verification and qualification processes.

3.1 PRODUCT ASSURANCE ORGANISATION

This subsection describes the structure, responsibilities, authority, and resources of the Product Assurance group as applied to software, as well as their interfaces with the software development effort.

3.2 PRODUCT ASSURANCE RELATIONSHIPS

This paragraph shall identify all PA groups (reliability, Quality Assurance, Safety, Configuration Management etc.) that are involved in product assurance tasks at any point in the software life-cycle. If the responsibility for certain product assurance tasks is allocated to groups not formally part of the PA organisation, they shall be included in this section. A chart or diagram shall be used to show the network of relationships and responsibilities.

3.2.1 Management and reporting structure

This paragraph shall identify the external authority and reporting relationships of the PA organisation with respect to both programme management and company or divisional management in a diagram. It shall define how information will be made available to programme management and how deficiencies, nonconformances, and proposed improvements will be brought to the attention of management. The interfaces of this plan to other programme plans shall be identified.

This paragraph shall also identify the internal structure of the Product Assurance organisation. The responsibilities, reporting and interfaces of those organisational elements which contribute to the SPA activity shall be defined in a chart or diagram. Those PA organisational elements which do not contribute to the SPA activity shall be identified as noncontributing groups.

3.2.2 Responsibilities

This paragraph shall describe the responsibilities of the Product Assurance group which assist in achieving the objectives of the software development programme.

3.2.3 Documentation

This paragraph shall identify the documentation produced by the SPA group regarding software. It shall state how the documents are to be checked for adequacy and identify the method by which this check is performed.

3.N [PA DISCIPLINE N] ORGANISATION

This section shall be numbered sequentially starting from 3.3 and shall address in turn each of the PA discipline groups identified in Section 3.2. The internal structure, authority and resources of that resource group applied to assuring software and their interfaces with the development effort should be described as defined below.

3.N.1 Management and reporting structure

This paragraph shall identify the relationships of authority and reporting of the resource group with respect to the management reporting channels identified in Section 3.2.1. This paragraph shall also identify the internal structure of the discipline group.

3.N.2 Responsibilities

This paragraph shall describe the responsibilities of the discipline group which assist in achieving the objectives of the Software Product Assurance programme.

3.N.3 Personnel

This paragraph shall identify the number and skill levels of personnel that will perform Software Product Assurance tasks. The personnel shall be described by title and minimum qualifications for the position.

3.N.4 Resources

This paragraph shall describe the specific resources necessary for performing the group's SPA tasks. The description of each resource shall reference the paragraphs in Section 5.0 defining the SPA activities which require that resource.

3.N.5 Documentation

This paragraph shall identify the documentation produced by this group regarding the software product assurance activities performed by this group. It shall state how the documents are to be checked for adequacy and identify the method by which this check is performed.

4.0 PA PROCEDURES, METHODS, TOOLS, AND FACILITIES

This section shall identify and describe all procedures, methods, tools, and facilities that will be used to assure the software and associated documentation and activities. This shall include identifying the tools, procedures, and facilities used to verify and/or qualify the software. Descriptions of methods and methodologies shall include the name and identification of source material. Descriptions of procedures and tools shall include the name, identification number, and version identification of each and its role in the product assurance process. Some or all of this information may be provided by reference to appropriate sections of company or programme Standards and Procedures Manuals.

5.0 SOFTWARE PRODUCT ASSURANCE ACTIVITIES

This section shall describe all SPA activities performed during the software life-cycle. This section shall contain the following paragraphs. Each paragraph shall identify the procedure for each activity, the documentation produced by that activity, the distribution of the information, the frequency of occurrence, and the allocation of activities and tasks to the specific resource groups identified in Section 3.0.

5.1 PHASE-INDEPENDENT ACTIVITIES

This paragraph shall describe the product assurance activities that will occur during all phases of the software development cycle. Each subparagraph shall identify the assessment criteria to be used and the assessment methods and tools to be employed.

5.1.1 Assessment of plans, standards, procedures, tools and facilities.

This paragraph shall describe the activities and plans to assess all software plans and procedures, including the Software Management Plan, the Configuration Management Plan, the Software Standards Manual, the Qualification Plan, the Verification and test plans, the Software Product Assurance Plan, and updates to these documents to determine whether the selected methodologies, standards, procedures, tools and facilities are in compliance with contractual requirements and are adequate to support the software development programme.

5.1.2 Assessment of configuration management

This paragraph shall describe the plans and activities for evaluating the configuration management system applied to all elements throughout the software life-cycle. It shall include plans for evaluating configuration identification, configuration control, configuration status accounting and reporting, and preparation for configuration audits.

5.1.3 Assessment of software development library

This paragraph shall describe the plans and activities to assess the library used for configuration management during the development of software (before the latter is formally baselined). It shall include plans for evaluating the content, procedures, controls, and status accounting and reporting mechanisms provided by the library.

5.1.4 Assessment of documentation and media distribution

This paragraph shall describe the plans and activities for evaluating the control and distribution of documentation and software media. It shall include plans for evaluating the controls assuring use of complete, consistent, and up-to-date information by members of the software programme.

5.1.5 Assessment of storage and handling

This paragraph shall describe the plans and activities for evaluating the system of storing and handling of software media and documentation. It shall include be plans for evaluating protection of materials, security of data, and backup procedures.

5.1.6 Assessment of nondeliverables

This paragraph shall describe the plans and activities to assess the nondeliverables used on the programme. It shall include plans for evaluating compliance with applicable contractual requirements and adequacy of configuration management of nondeliverables.

5.1.7 Assessment of risk management

This paragraph shall describe the plans and activities to assess the procedures employed and the results achieved by risk management on the programme.

5.1.8 Assessment of subcontractor products

This paragraph shall describe the plans and activities for assuring that software and documentation received from subcontractors conform to contractual requirements. It shall include plans for evaluating pre-award surveys of prospective subcontractors, adequacy of requirements established for subcontractors, adequacy of subcontractor procedures as planned and as implemented, and adequacy of subcontractor products.

5.1.9 Assessment of reusable and customer furnished software

This paragraph shall describe the plans and activities to assess the planning performed for the use of reusable, commercially available, and customer furnished software. It shall also describe the plans and activities to assess this software, once acquired, and for certifying that reusable software meets specified criteria.

5.1.10 Software product assurance records

This paragraph shall describe the plans and activities to prepare and maintain records for each software product assurance activity. It shall identify the formats to be used and the information to be recorded for each activity. It shall identify plans and activities to assess the records, maintain them for internal use, and to make them available for customer review.

5.1.11 Assessment of software corrective action system.

This paragraph shall describe the plans and activities to assess the corrective action system applied to the software. It shall include plans and activities to assess:

1) reporting of detected nonconformances;
2) analysis of reported nonconformances;
3) classification of nonconformances by category and priority;
4) identifying necessary corrective action
5) identifying trends in reported nonconformances
6) analysis of these trends to recommend changes to improve software quality;
7) authorising implementation of corrective actions;
8) documenting the corrective actions taken;
9) performance of re-assessments after corrections have been made;
10) tracking and closing out corrected nonconformances, and;
11) providing visibility to the customer into critical nonconformances based on the categorisation and priority schemes used in the reports.

5.1.12 Assessment of software assessment system

This paragraph shall describe the plans and activities to assess the effectiveness of the assessments of software performed by SPA.

5.1.13 Certification

This paragraph shall describe the plans and activities for providing evidence that tools and the deliverable products are in compliance with contract requirements.It shall include a description of the evidence that will be presented in support of the certification.

5.1.14 Interface with independent verification and validation contractor

This paragraph shall describe the plans and activities for interfacing with the Independent Verification and Validation (IV&V) contractor, if applicable. It shall include plans and activities to provide the IV&V contractor with materials to be assessed, processing nonconformance reports submitted by the IV&V contractor, participation in meetings, and coordinating on the status of the reported nonconformances.

5.1.15 Customer review

This paragraph shall describe the plans and activities for providing the contracting agency with facilities and access for reviews of

products and activities at contractor, subcontractor, or vendor facilities.

5.1.16 Quality cost data

This paragraph shall describe the plans and activities to collect, analyse, and document data relative to the cost of detecting and correcting problems in the software and associated documentation. It shall identify the specific cost data to be collected and the analysis to be performed on that data.

5.2 PHASE DEPENDENT ACTIVITIES

This section shall contain subsections, each of which deals with a specific life-cycle phase.

5.2.X (Phase x name) assessment activities

This subsection shall be numbered sequentially starting from 5.2.1 and shall address each of the life-cycle phases in turn with the following subparagraphs.

5.2.X.1 Activities assessment

This paragraph shall describe the plans and activities to conduct reviews, audits, and assessments of software work processes to determine their compliance with approved plans, procedures, standards, and specifications. This shall include assessment of the planning, preparation, and execution of the assessment activities to be conducted during this phase. The description shall identify the activities to be assessed, and for each, the assessment criteria, methods, tools, and responsible resource group as identified in Section 3.0.

5.2.X.2 Product assessment

This paragraph shall describe the plans and activities to conduct reviews, audits, and assessments of software work products to determine their compliance with approved standards, specifications, and configuration data. This shall include assessment of the planning, preparation, and execution of the evaluation activities to be conducted during this phase. The description shall identify the products to be assessed, and for each, the assessment criteria, methods, tools, and responsible resource group as identified in Section 3.0. Assessment criteria shall include, as a minimum, adherence to the required format, compliance with contractual requirements, traceability to and consistency with other software development products as appropriate, internal consistency, understandability, technical adequacy, and appropriate degree of completeness.

5.3 QUALIFICATION

This paragraph shall describe the plans, activities, and procedures for supporting the qualification of the software.It shall include plans for ensuring that the qualification requirements are complete, that the qualification programme is properly planned and executed, and for maintaining the qualification status of the design after changes to the system baseline.

5.4 ACCEPTANCE INSPECTION

This paragraph shall describe the plans and activities for supporting customer acceptance inspection.It shall include plans for ensuring that all required products will be available and ready for customer inspection, all required procedures have been performed, and that evidence from these procedures will be available for customer inspection.

5.5 INSTALLATION AND CHECKOUT

This paragraph shall describe the plans and activities for assessment of the installation and checkout of the software, if required by the contract, to ensure that this activity has been carried out in compliance with the procedures specified in the software development plans.

6.0 SCHEDULE

This section shall identify the schedule for all SPA activities and milestones with reference to the master schedule for software development activities and milestones. For each activity, the schedule shall indicate the activity initiation, dependencies on other activities or events, and activity completion times. Key development milestones such as formal reviews, audits, and meetings shall be shown. The schedule should be described graphically.