SST Programme: Product Assurance and Quality Plan

SST-PRO-PLA-005

Version 2a

Prepared by:		
Nicola La Palombara (INAF)	Nicola La Palombara	SST-PRO PRQM
Latest Release Checked by:		
Alessio Trois (INAF)	Alessio Trois	SST-PRO PRM
Salvatore Scuderi (INAF)	Salvatore Scuderi	SST-STR PM
Jean-Laurent Dournaux (OP-INSU)		SST-FRC PM
Richard White (MPIK)		SST-CAM PM
Fatima De Frondat LAADIM (OP-INSU)		SST-PRO PRRM
Approved by:		
Gianpiero Tagliaferri	Gianpiero Tagliaferri	SST-ESC

Current Release				
Ver.	Created	Comment	Distribution	Editor(s)
2a	28/07/2023	Updating and Re-issuing of document following the outcome of the Product Review	SST Consortium	N. La Palombara (INAF)

Version History				
Ver.	Created	Comment	Distribution	Editor(s)
1a	14/10/2021	Updating and Re-issuing of DVER document: SSTER-SST05-QP dated 5/6/2020	SST Consortium	N. La Palombara (INAF)
1b	14/11/2022	Updating and Re-issuing of document for the Product Review	SST Consortium	N. La Palombara (INAF)
2a		Updating and Re-issuing of document following the outcome of the Product Review	SST Consortium	N. La Palombara (INAF)

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Overview

The small-sized telescopes (SSTs) will be provided as an in-kind contribution (IKC) for the southern site (CTA-S) of the Cherenkov Telescope Array Observatory (CTAO). According to the SST Programme Project Management Plan [AD1], the SST Programme is composed of six different main work packages (WPs): the programme office (SST-PRO, WP 1000), the telescope structures (SST-STR, WP 2000), the telescope mechanics (SST-MEC, WP 3000), the telescope optics (SST-OPT, WP 4000), the telescope control system (SST-TCS, WP 5000), and the telescope cameras (SST-CAM, WP 6000). SST-PRO manages and coordinates all the SST Programme, while SST-STR and SST-CAM are two distinct Projects aimed to provide a deliverable or set of deliverables to SST-PRO. Each Project is under the responsibility of a Project Lead Partner: INAF for SST-STR and MPIK/MPG for SST-CAM. In turn, SST-STR controls and manages the realization of all the activities related to the subsystems SST-MEC, SST-OPT, and SST-TCS. In particular:

- the overall telescope structures (WP 2000) and control system (WP 5000) are directly provided by INAF and OP-INSU as IKC
- the cameras (WP 6000) are directly provided by MPIK/MPG as IKC
- the telescope mechanics (WP 3000) an optics (WP 4000) are provided by Industrial Partners, which are involved into the SST Programme through specific commercial contracts, awarded by INAF on the basis of public tenders

The WPs under the direct responsibility of a Lead Partner are considered as internal suppliers, while those under the responsibility of an Industrial Partner are considered as external suppliers. As regards the external suppliers, SST is a purchaser-like.

Each project or subsystem is internally organised, but at a minimal level comprises a set of Work Packages under the coordination of a Project Manager. In addition, each Project or subsystem will contain a Quality Manager and a System Engineer (the only exception is the TCS, which does not include a QM). Project roles are appointed by the Project Partners in the manner most appropriate for the specific needs of that SST Project or subsystem.

1.2 Purpose

This document describes the general quality requirements, activities, methods and required resources applicable to all the Work Packages (WPs) of the SST programme, projects and subsystems, with the aim to meet the quality objectives and to assure the expected performance and reliability.

This quality plan will provide assurance that:

- The CTA SST items in all their parts are compliant with the specifications
- The risks are identified, assessed and controlled
- The traceability and quality of deliverables are accessible at all times
- Non-conformities (NCs) are identified and addressed

This quality plane is:

- Written and updated by the Programme Quality Manager (QM)
- Approved by the SST Programme Office (SST-PRO)
- Implemented by the SST Project Office coordinators with the help of the QM

It is responsibility of each SST Project to implement this quality plan, while each external supplier is responsible for creating and implementing its own quality plan according to its internal organization, products, processes, and phase of the SST Programme in which it is involved. Each quality plan should describe how quality is managed within its constituent organization and how the required activities will be carried out, either in the quality plan itself or by reference to appropriate documented procedures or other documents. These quality plans and referenced documents shall be made available to the SST-PRO.

These specific quality plans should include the following:

1. All aspects contemplated in this SST quality plan or, in special cases, well-founded reasons for excluding certain aspects of the present document.
2. Responsibilities and authorities of the persons involved in the design and production of the contributed items during the different project or subsystem phases.
3. Allocation of resources, manpower, training, equipment, etc. necessary for quality-related activities.
4. Quality assurance activities for the product design.
5. Quality assurance and quality control activities for production.
6. Sequence of events, key dates and hold points.
7. List of quality records to be retained.
8. Reference to the documented change-control procedure.
9. Quality requirements for procurement which should be negotiated and agreed with the suppliers.
10. Necessary testing, controls, inspections and audits for each phase of the project or subsystem.
11. Method of identification and traceability of items.
12. Internal control procedure of nonconforming items.

1.3 Scope

The contents of the present PA plan are fully applicable to each supplier and subcontractor. Each subcontractor shall provide a compliance statement to the plan at the beginning of the contract.
This document is applicable to the design, construction, and installation phases of the SST telescopes, up to the telescope delivery to CTAO.

1.4 Content

This document is organised as follows:

- Section 2 provides an overview of the Product Assurance programme for the SST programme and projects and subsystems.
- Section 3 provides an overview of the Risk control
- Section 4 provides the general Quality Assurance requirements, which are applicable to both the internal and external suppliers of the SST Projects and regard both hardware and software items
- Section 5 provides the specific Quality Assurance requirements for the acceptance of the deliverable items, which apply to both internal and external suppliers of the SST Projects and regard both hardware and software items
- Section 6 describes the Quality Assurance programme specific for hardware items, which is applicable to both the internal and external suppliers of the SST Projects
- Section 7 provides an overview of the Quality Assurance programme specific for software items, which is applicable to both the internal and external suppliers of the SST Projects
- Section 8 describes the management of the non-conformances; it is applicable to both the internal and external suppliers of the SST Projects and regards both hardware and software items

- Section 9 provides an overview of the approach to the RAMS analysis, which will be described in a specific document

1.5 Applicable Documents

[AD1] SST Programme: Programme Management Plan - SST-PRO-PLA-001

[AD2] CTA Construction Project Quality Plan - MAN-QA/110405 v. 2.1, 26 October 2015

[AD3] SST Programme: Configuration And Data Management (CADM) Plan – SST-PRO-PLA-002

[AD4] Risk Management Plan - SST-PRO-PLA-004

1.6 Reference Documents

[RD1] SST System Safey Management Plan - SST-PRO-PLA-006

1.7 General Specification and Standard Documents

[SD1] Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on Machinery, and amending Directive 95/16/EC

[SD2] MILITARY HANDBOOK: ELECTRONIC RELIABILITY DESIGN HANDBOOK - MIL-HDBK-338B

[SD3] MILITARY HANDBOOK: RELIABILITY PREDICTION OF ELECTRONIC EQUIPMENT- MIL-HDBK-217F

[SD4] Basis of Structural Design - EN Eurocode 0

[SD5] Steel – Design of Steel Structures – All parts - EN Eurocode 3

[SD6] Design of Composite Steel and Concrete Structures – All parts - EN Eurocode 4

[SD7] Design of Aluminium Structures – All parts - EN Eurocode 9

[SD8] Safety requirements for electrical equipment for measurement, control, and laboratory use - Part 1: General requirements - EN 61010-1

[SD9] Safety of machinery, Functional safety of safety-related electrical, electronic and programmable electronic control systems - EN 62061,

[SD10] Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design - EN ISO 13849-1

[SD11] Safety of Machinery – Emergency Stop – Principles for design - EN ISO 13850

[SD12] Low-voltage electrical installations - EN 60364 series

[SD13] Basic and safety principles for man-machine interface, marking and identification - Identification of equipment terminals, conductor terminations and conductors, 2010 - EN 60445,

[SD14] Insulation coordination for equipment within low-voltage systems - EN 60664 series,

[SD15] Reliability Modelling and Prediction reference - MIL-STD-756B

[SD16] System Safety - MIL-STD-882E

[SD17] Procedures for performing a Failure Mode, Effects and Criticality Analysis reference - MIL-STD-1629A

[SD18] EMC Directive 2004/108/EC

[SD19] Electromagnetic Compatibility (EMC) - EN 61000 series

[SD20] Functional Safety and IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems

[SD21] IEC 61131-3, Programmable controllers - Part 3: Programming languages

[SD22] Lightning protection standard - EN 62305:2011

[SD23] Cleanrooms and associated controlled environments - Part 1 - ISO 14644-1:2015

[SD24] ECSS-Q-ST-80C Rev.1 - SW Product Assurance (15 February 2017)

[SD25] ECSS-Q-ST-10-04C - Critical Item control (31 July 2008)

[SD26] CTAO Software Licensing Policy - CTA-STD-OSO-000000-0002

[SD27] Software Programming Standards - CTA-STD-OSO-000000-0001

[SD28] CTAO System Control Standards - CTA-STD-SEI-000000-0004

1.8 Definition of Terms and Abbreviations

ABCL	As-Built Configuration List
ADCL	As-Designed Configuration List
ADP	Acceptance Data Package
AIT	Assembly Integration and Testing
AIV	Assembly Integration and Verification
APM	AIV/AIT Project Manager
AR	Acceptance Review
ASAP	As-soon-as-possible
BKO	Bridging phase Kick-Off
CADM	Configuration and Data Management
CDR	Critical Design Review
CI	Configuration Item
CIDL	Configuration Item Data List
CIL	Critical Item List
COTS	Commercial Off The Shelf
CPM	Camera Project Manager
CTA	Cherenkov Telescope Array
CTAO	Cherenkov Telescope Array Observatory
DR	Delivery Review
DVER	Design Verification Engineering Review
ECR	Engineering Change Request
EEE	Electrical, Electronic and Electromechanical
EIDP	End-Item Data Package
ERIC	European Research Infrastructure Consortium
FAR	Final Acceptance Review
FMEA	Failure Mode Effects and Analysis
FMECA	Failure Mode Effects and Criticality Analysis
GSE	Ground Support Equipment
IACTs	Imaging Atmospheric Cherenkov Telescopes
IKC	In Kind Contribution
INAF	Istituto Nazionale di Astrofisica
KIP	Key Inspection Point
KO	Kick-Off

MAIT	Manufacturing, Assembly, Integration and Test
MIP	Mandatory Inspection Point
MPIK	Max-Planck-Institut für Kernphysik
MTBF	Mean Time Between Failure
OP	Observatoire de Paris – PSL, CNRS
NC	Non-Conformance
NCR	Non-Conformance Report
NRB	Non-Conformance Review Board
PA	Product Assurance
PAR	Provisional Acceptance Review
PBS	Product Breakdown Structure
PDR	Preliminary Design Review
PFMEA	Process Failure Mode Effects and Analysis
PMP	Programme Management Plan
PO	Project Office
PQR	Production Qualification Review
PR	Product Review
PRM	Programme Manager
PSE	Programme System Engineer
PSL	Paris Sciences et Lettres
QA	Quality Assurance
QM	Quality Manager
RAMS	Reliability, Availability, Maintainability, and Safety
RFD	Request For Deviation
RFW	Request For Waiver
SDT	SW Development Team
SE	System Engineer
SOW	Statement Of Work
SPAP	Software Product Assurance Plan
SPM	Structure Project Manager
SST	Small Size Telescope
TRR	Test Readiness Review
VCD	Verification Control Document
WBS	Work Breakdown Structure
WP	Work Package
WPD	Work Package Description

2 Product Assurance programme

The present document defines the Product Assurance programme to be implemented by the partners of the SST Programme.

To fulfil the PA requirements applicable to the SST Programme, the suppliers shall maintain an established PA programme, explained in this document.

In particular, the PA Programme has the following tasks:

- To assure and verify that performance and quality requirements are properly fulfilled by the design and the products;
- To assure that the design, development and verification processes are compliant with the QA requirements;
- To apply the necessary control during throughout the Design, Manufacturing, Assembly, Integration and Qualification/Acceptance Testing for the achievement of the required quality level.

2.1 Product Assurance programme planning

2.1.1 Product Assurance organization, roles, and responsibilities

According to the SST Programme Project Management Plan [AD1], all the Product Assurance (PA) activities described in this PA Plan will be coordinated by the Programme Quality Manager (PRM-QM). The PRM-QM, who reports directly to the Programme Manager (PRM), is responsible for the coordination of the Product/Quality Assurance activities for the SST Programme as well as the Projects and subsystems (WP 1300). He/She is the CTAO first contact point for Quality activities and negotiates and / or reports on any topic related to these activities. He/She has to establish and control an effective Quality Management Plan covering:

- Quality and Product Assurance plan.
- Control of the selection of materials, processes, EEE components and mechanical components
- Approval of no conformity, waiver/deviation from the Projects
- Management of no conformity, waiver and deviation with respect to the CTAO
- SST-PRO Configuration Management.

In the frame of the SST organization, the authority and responsibility for Product Assurance is placed under the jurisdiction of the Programme QM, for all the duration of the project. The PRM-QM has direct access to the company's or Institute’s top management for regularly reporting on the PA programme status. The Programme QM shall report to the PRM the status of the PA activities and shall have organizational authority to establish and implement the applicable PA programme.

The Programme QM is responsible for the following main activities:

- management of PA tasks;
- implementation and maintenance of the programme PA defined in the PA plan;
- verification that required PA activities are covered;
- survey, audits of personnel, procedures and operations implemented in the frame of project;
- reporting and documentation of the PA activities as defined in the contract;
- implementation of non-conformance processing system;
- identification and resolution of inconsistencies between Product Assurance applicable documents;
- control of PA schedule and cost;
- control of Supplier PA activities.

The coordination of all the activities regarding reliability, availability, maintenance and safety (RAMS) will be under the responsibility of the Programme RAMS Manager (PRM-RAMS), who defines the RAMS policy and specifications, manages this activity and ensure that the projects and subsystems meet the CTA requirements (WP 1400). The PRM-RAMS is the CTAO first contact point for RAMS activities and negotiates and / or reports on any topic related to these activities.

The PRM-QM and the PRM-RAMS will provide support to each other:

- On one hand, the PRM-RAMS will act as deputy PRM-QM
- On the other hand, the PRM-QM will act as deputy PRM-RAMS

The deputy PRM-QM supports the PRM-QM for the main tasks below:

- Organization and management of the PA/QA activities and PA/QA Team,
- Participation to the preparation of the SST reviews and to these reviews

The deputy PRM-QM is the CTAO second contact point for Quality activities and negotiates and / or reports on any topics related to these activities. The deputy PRM-QM assists the PA/QA Manager for the tasks below:

- To answer the PA/QA RIX
- To define a methodology to manage and control the project documentation
- To record and manage non-conformities with the project team
- To control that the different activities (design, tests, calibrations, etc.) are properly documented
- To control subcontractors and monitor the sub-contracted activities following what was defined and agreed in contract
- To define the criteria for product acceptance with the project team

The PRM-QM and the deputy PRM-QM coordinate the activities of the Projects and subsystems QMs. Each Project or subsystem QM is responsible for the coordination of the Product Assurance/Quality Assurance activities of his/her Project. Project and subsystem QM responsibilities include:

- Project Quality and Product Assurance.
- Project Reliability
- Project Maintainability
- Identification of project critical Item or process for reliability, maintainability, obsolescence, safety
- Selection in the project framework of materials, processes, EEE components and mechanical components
- Management of project no conformity
- Project Configuration Management

The deputy PRM-RAMS supports the PRM-RAMS for the organization and management of the RAMS activities and RAMS Team. The deputy PRM-RAMS is the CTAO second contact point for the RAMS activities and negotiates and / or reports on any topics related to these activities. The deputy PRM-RAMS assists the RAMS Manager for the tasks bellow:

- To answer the RAMS RIX
- To define a methodology to manage and control the RAMS documentation
- To control that the RAMS activities are properly documented

The PRM-RAMS and the deputy PRM-RAMS coordinate the activities of the Project and subsystem QMs to define a methodology to carry out and control RAMS activities.

The duties, responsibilities, tasks and interfaces of the PRM-QM, the PRM-RAMS, and the Project or subsystem QMs are defined in the SST Project Management Plan [AD1].

The implementation of the PA/QA requirements will be in charge of the industrial partners or suppliers responsible for the manufacturing, assembly, integration and test (MAIT) activities, which shall appoint a specific person as Product Assurance and Quality Assurance manager. Each PA manager is responsible for the implementation of all the Product and Quality Assurance tasks described in this PA Plan in its own organization and for each sub-contractor and supplier of its competence. The monitoring and verification of this implementation, at Programme and Project levels, will be in charge of the respective QMs.

The PA managers of the industrial partners or suppliers, supported by specialists or dedicated resources as necessary, shall be responsible for the following disciplines:

1. Quality assurance
2. EEE components
3. Materials, Mechanical Parts and Processes
4. Dependability and Safety analyses
5. SW product/quality assurance

2.1.2 Product Assurance interfaces

The QM of each SST Project shall interface with the relevant internal and external suppliers regarding all the PA matters.

2.1.3 Product Assurance plan

Each supplier, either internal or external, shall prepare, maintain and implement a plan of the PA activities in agreement with the SST PA requirements.

2.2 Product Assurance programme implementation

The implementation of the Product Assurance programme will be addressed by the following principles:

- to ensure the allocation and availability of adequate resources, personnel and facilities to carry out the required PA tasks;
- to define all the PA activities consistent with the Project objectives, requirements, criticalities and constraints;
- to ensure that lower level contractors / suppliers perform proper PA monitoring and control;
- to 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;
- to support the risk assessment and control including evaluation of the acceptability of the residual ones;
- to support configuration management.

2.2.1 Product Assurance management

The Programme QM shall ensure that the inputs to perform the PA activities are consistent and complete, and available in line with the project schedule, and that the outputs produced by the PA activities are consistent and complete, and delivered in line with the project schedule. Moreover, the Programme QM shall ensure that all the tasks described in this PA Plan are performed in line with the project schedule.

The Programme QM shall control the quality of products provided by the internal or external suppliers by issuing applicable PA requirements and ensuring their implementation. The Programme QM shall ensure that a qualification programme is defined, approved, implemented and maintained by the relevant organization.

The Programme QM shall approve the product acceptance during the Acceptance or Delivery Review.

2.2.2 PA reporting

The internal and external suppliers shall report on the status and progress of the PA programme implementation. The PA report shall include at least the following items for the reporting period:

- Progress and accomplishment of each major PA task, including resolved and new problems, future planning of major activities and events
- Status of PA reviews, Audits, Mandatory Inspection Points (MIPs), Key Inspection Points (KIPs), Waiver requests, Non-conformances (minor and major), Critical items (including mitigation action plan status), Qualification status, EEE component status, Material and processes status, Alerts status.

The PA progress report may be part of the project or subsystem progress report.

2.2.3 Documentation and data control

Product Assurance documentation will include at least:

- product assurance plan;
- product assurance requirements to suppliers;
- critical items list (CIL);
- dependability and safety analyses;
- EEE component documentation;
- Materials, Mechanical Parts and Processes documentation;
- software quality assurance documentation;
- inspection and audit reports;
- End Item Data Package (related to PA documentation);
- Configuration Item Data List (CIDL);
- major non-conformance/failure reports (NCR);
- non-conformance status record book;
- RFD/W;
- quality records;
- Certificate of Conformity

Quality records will provide objective evidence of complete performance of QA tasks and will demonstrate achievement of the required quality level. They will be stored in safe conditions which prevent alterations, loss or deterioration and will be retained for the period defined in the requirements and specified in the commercial contracts signed between external suppliers and Lead Partners. They will be readily accessible and retrievable whenever they are needed.

The expected delivery of these documents, at various reviews, shall be defined according to the applicable business agreements.

The documentation and data management shall be performed according to the SST Documentation and Data Management Plan **Error! Reference source not found.**.

The Programme QM shall ensure that the applicable issues of all documents and data are available at all locations where activities required for the implementation of the PA programme are performed.

The Programme QM shall ensure that invalid or obsolete documents and data are removed from all points of issue or use or assured against unintended use.

The SST Project Control Manager, whose role is defined in the SST PMP [AD1], shall ensure that obsolete documents and data retained for legal or knowledge preservation purposes are identified as such. These documents shall be maintained in the SST Data Management System **Error! Reference source not found.**.

The Programme QM, in collaboration with the PRM, shall identify the project documents requiring approval, including those requiring approval by QM.

2.2.4 Reviews and Reporting

Reviews are carried out throughout the project life cycle, according to the SST PMP [AD1] and the business agreements with industrial partners, at all levels from mission to unit level. Project reviews are examinations of the technical status of a project or subsystem and associated issues at a particular point in time. Their primary purpose is to provide a comprehensive assessment of the project status against targets and requirements.

The status and the progress of the PA programme shall be reported on a periodic and systematic basis. Exceptional reporting shall occur when urged by non-routine events, like failure of items during manufacturing or testing.

2.2.5 Personnel and Certification

Training programme for personnel whose performance determines or affects product quality and certification of personnel, involved in critical processes and operations, will be performed and assured, under proposal of management, for the whole supply chain. Verification of aptitude to perform the work will be performed through consideration of capability and experience.
The QA team is responsible to verify that all personnel involved in critical processes, critical operations and inspections activities, are properly trained, certified and periodically re-certified or verified.

2.2.6 PA contribution to configuration management

The configuration management is closely linked to the PA management. Therefore, the Programme QM shall ensure that:

1) the as-designed status is defined and released prior to manufacturing;
2) the as-built documentation is properly defined, identified and maintained in order to reflect approved modifications;
3) items to be delivered comply with the as-built documentation.

2.2.7 Non-conformance control

The Programme QM shall establish and maintain a non-conformance control system, as described in Section 8 of this document.

3 Risk control

The PA/QA function will contribute to the overall risk management activities by:

- Supporting the identification and risk evaluation of critical items for which major difficulties or uncertainties are expected in:
  - instrument interface compliance;
  - demonstration of design performances;
  - development and qualification of new product, processes and technologies;
  - procurement, manufacturing, assembly, inspection, test, handling;
  - storage, handling and transportation, which may lead to major degradation in the scientific performance of the instrument;
  - human-related issues, regarding e.g. personnel hired with fix term contracts, team making, free choice of research for staff personnel
- Contributing to the risk reduction plan by identifying the QA activities accompanying the individual risk reduction measures.
- Monitoring and documenting the achievement of the specified risk reduction implementation and the corresponding verification measures throughout all project or subsystem phases.
- Identifying single-point failures with a failure consequence severity classified as catastrophic, critical or major (Reliability Critical Items).
- Identifying items or procedures that do not comply with the applicable safety requirements, or which cannot be verified as complying with those requirements (Safety Critical Items).
- Identifying products that cannot be checked and tested after integration, limited-life products, products that do not meet – or cannot be verified as meeting – applicable maintainability requirements (Maintainability Critical Items).
- Identifying items whose structural failure may cause catastrophic or critical consequences (Fracture Critical Items).

All members of the project team are responsible to identify and manage risks that might arise.

The risk assessment is based on the qualitative and quantitative analysis of the identified risk as follows:

- To identify the milestone(s) of the project or subsystem that are negatively affected by risk occurrence;
- To identify any direct impact in terms of adverse events on time (schedule), cost, and performance.

A risk factor is attributed to each identified risk in order to explore priorities of the related action plans.

The risk analysis covers the following domains:

- technical documents
- architecture/design and development (including single point failures, Elements with limited life characteristics, critical parts, qualification of new product, processes and technologies …)
- manufacturing, assembly, testing (including heritage, handling, specific constraints, test benches, software…)
- development plan/schedule management
- contract/financial/cost.

4 General Quality Assurance requirements

The content of this section applies to both the internal and external suppliers of the SST Programme and regards both hardware and software items.

4.1 QA requirements for design and verification

4.1.1 Design rules

Any product shall be designed such that it can be produced with the specified level of quality, its performances and characteristics can be reproduced over different models and serial production, it can be inspected and tested under representative conditions (for production, AIV and operational environment), and it can be operated in accordance with programme constraints and requirements, throughout its whole life cycle (including handling, storage, transportation, integration and operations).
Coordinated QA actions will be planned throughout the design and development phases in order to assure that functional and technical requirements are consistent and that the design will fulfil the requirements.
QA personnel will ensure that the design rules and guidelines related to producibility, repeatability, inspectability, testability and operability are properly implemented in the design.
The relevant actions will include:

- a close survey of the adequacy of design and development documentation;
- the performance assessment of design reviews in line with the contract;
- the critical items control plan;
- the approval of design verification matrix;
- the qualification testing witnessing;
- the safety program plan;
- the dependability program plan;
- the software quality assurance program plan

Any change performed to an agreed design will be properly identified, documented, justified, scheduled and submitted to new agreement before implementation.
Basic design rules are:

- Producibility – avoid design features that are too difficult to manufacture, pose integration/disassembly or interface problems.
- Tolerance control – stack-up method to be clear.
- Repeatability – design should allow for tolerances to make other identical units similar in performance
- Inspectability – parts or assemblies should be accessible. Not always possible; when future access is to be lost, Mandatory and Key Inspection Points (MIP/KIP) should be planned.
- Testability – test points to be included to allow for fault identification
- Operability – limit the constraints to hinder operations during ground testing, or provide as part of the design the necessary Ground Support Equipment (GSE) or test mode to avoid this limitation.

The PA responsible shall contribute to the verification of the design and of its consistence with requirements by issuing a series of documents and analysis: Reliability Analysis, Part Stress Analysis (PSA), FMECA, Declared Component List (DCL), Declared Material List (DML), Declared Mechanical Part List (DMPL), Declared Process List (DPL), Worst Case Analysis (WCA).
All these documents shall be issued at the design reviews described in the SST PMP [AD1] and updated according to design development. These documents shall be based on the engineering design documentation verified at the internal design meetings with project group.

4.1.2 Critical Items identification and control

The goal of Critical Item management is to list items that may present particular problems to the project or subsystem, to define steps to reduce the probability of those problems occurring, and to implement effective controls. Critical Items will be considered following these criteria:

- items not qualified
- items which are difficult to test
- items containing limited life parts (i.e., wear-out modes) in the frame of the project or subsystem
- items using not qualified, new or modified technologies
- items causing critical or catastrophic hazards
- single point failures that could produce unacceptable downtime of the instrument for corrective maintenance
- failures with risk of propagation (at upper level or to internal redundancy)
- non-standard processes

The results of design analyses and other sources - such as, for example: Worst Case Analysis, Part Stress Analysis, Fault Tree Analysis, Failure Mode and Effect Analysis, Safety Analysis, etc. - shall be used as input data for the preparation of the list.

According to ECSS standard [SD25] the Critical Item List (CIL) shall provide, as a minimum, the following data:

- configuration item identification;
- descriptive name;
- reason for criticality;
- control program proposed;
- criticality status.

The complete CIL will be updated to the main reviews and will be maintained permanently, changes will be reported as part of the progress report and during the progress meetings.

The process of Critical Items identification will start early in the design/development phases and its objectives are to:

- define the characteristics of the critical item, once it has been found that the elimination of it is not immediately possible;
- derive requirements for the supplier for what concerns the manufacturing, integration and test of the item itself;
- identify in the user manual any special precaution or constraint for the AIT at higher levels;
- implement the necessarily precautions, prior to starting the manufacturing of the first standard equipment in which they have to operate.

4.1.3 Deviations and Waivers

In some cases, it might be necessary and perhaps feasible to supply a non-conforming product. In such cases, a Request For Waiver (RFW) or a Request For Deviation (RFD) shall be issued by the supplier (either internal or external) in order to collect the authorisation of the SST-PRO.

4.1.3.1 Deviation

A deviation occurs when the product does not meet the requirements or specifications before it has been produced (for example, a failure in the design has been detected), or when there is known evidence in advance that it will not meet the requirements once it has been produced (when the production process has a known problem) but for some reason the production must continue (for example, due to schedule constrains).

4.1.3.2 Waiver

A request for waiver is a request for authorization to accept an item which, during manufacturing or after final inspection, is found to depart from specified requirements but nevertheless is considered suitable for use as it is.

4.1.4 Verification rules

Verification activities provide objective evidence that the designs meet their specified requirements and that any non-compliance is identified. The suppliers will be required to demonstrate compliance of units, assemblies, and subsystems with specified requirements, according to their relevant development and qualification tests.

The requirement verification shall be performed progressively, as each stage of the project or subsystem is completed, and shall provide the organized base of data upon which qualification and acceptance is incrementally declared.

The top-down requirement allocations and bottom-up requirement verifications shall be complete and consistent.

A system for tracking requirements and verification of results shall be established and maintained during the whole project or subsystem life cycle.

The verification methods shall be adequate and consistent with the type and criticality of the requirements. Depending on the level and the product, the six different verification methods, adopted in CTA, can be envisaged, as listed in Table 4-1.

Table 4-1: CTA's adopted verification methods

Analysis (A)	Verification by Analysis (A) consists of the use of analytical data or simulations under defined conditions to show theoretical compliance. Analysis (including simulation) is used where verifying to realistic conditions cannot be achieved or is not cost-effective and when such means establish that the appropriate requirement, specification, or derived requirement is met by the proposed solution.
Certification (C)	Verification by Certification (C) consists of written assurance that the product or article has been developed and can perform its assigned functions in accordance with legal or industrial standards. The development reviews and verification results form the basis for certification; however, certification is typically performed by outside authorities, without direction as to how the requirements are to be verified. For example, this method is used for electronics devices via CE certification in Europe and UL certification in the United States and Canada. Note that verification methods prescribed by and within applicable standards take precedence over the verification methods described in CTA documents.
Demonstration (D)	Verification by Demonstration (D) consists of a qualitative exhibition of functional performance, usually accomplished with no or minimal instrumentation. Demonstration (a set of verification activities with system stimuli selected by the system developer) may be used to show that system or subsystem response to stimuli is suitable. Demonstration may also be appropriate when requirements or specifications are given in statistical terms.
Inspection (I)	Verification by Inspection (I) consists of performing an examination of the item against applicable documentation to confirm compliance with requirements. Inspection is used to verify properties best determined by examination and observation.
Review of design (R)	Verification by Review of Design (R) consists of using approved records or evidence that unambiguously show that the requirement is met. For example, design documents and reports, technical description documents, and engineering drawings.
Test (T)	Verification by Test (T) consists of an action by which the operability, supportability, or performance capability of an item is verified when subjected to controlled conditions that are real or simulated. These verifications often use special test equipment or instrumentation to obtain very accurate quantitative data for analysis.

These methods will be the ones adopted in the requirement specifications and verification plans. Verification activities shall be implemented since the early phase of the project and shall be reported through specific matrices (as compliance matrix, validation and verification matrix, etc.) according to the contractual documents, reflecting the status of design at each design review. PA/QA responsible shall verify regularly the progress of the different matrix completion.

The QA personnel shall participate in the review of hardware design and manufacturing activities to ensure compliance with control requirements and quality criteria. It shall be verified that parts and components are accessible for inspection after assembling.

Completely testability of hardware shall be verified during design development and, where not possible, relevant analysis shall be foreseen.

Any change performed to an already verified design shall undergo a new approved verification sequence.

Appropriate reference to the verification documentation shall be recorded and updated at project or subsystem reviews up to final acceptance.

4.1.5 Verification matrix

As result of the verification strategy, a verification matrix showing all requirements and their selected verification methods shall follow the progress in the project or subsystem development in all its phases from design to the acceptance.

4.1.6 Design reviews

According to the SST PMP [AD1], the major design reviews shall be the:

- Product Review (PR), which is an internal SST review organised by the SST consortium, with active participation from CTAO, in which the design of the projects/subsystems will be presented and any missing areas requiring further elaborations will be identified
- Critical Design Review (CDR), in which the final internally verified telescope design will be presented along with accompanying documentation and draft production plans.

Both reviews shall be conducted in accordance with project requirements and written procedures.

Design reviews shall assess that:

- Quality requirements and criteria for design, feasibility, standardization of parts and interfaces (if possible), repeatability, testability and operability are adequately considered in design documentation.
- Methods and data required for procurement, manufacturing, inspection and test are available and validated.
- Risks of not achieving requirements are highlighted and adequately controlled.

4.1.7 Documentation control

The following documents shall be recorded and stored by each QM:

- Technical Specifications
- Technical Design reports
- Detailed designs
- Manufacturing dossier
- Inventory list
- Interface Control Documents
- AIT/AIV plan
- Test plans
- Test procedures
- Test results in form of a Test Report
- Control plans
- Control and inspection results during and after production
- Non-conformance reports and corrective action plans
- User manual
- Installation and maintenance manual

In addition, a resume of the performed activities should be sent regularly to the SST-PRO.
The Raw Data obtained from tests, controls, and inspections shall be recorded and stored in the SST DMS [AD3].
Each QM, in collaboration with the Project Control Manager [AD1], shall audit regularly that:

- The documents of the SST projects or subsystem are controlled.
- Only the last approved version is available to the internal and external suppliers of the SST projects.
- The document references, histories, and approval status are correct and consistent.
- The documents are stored in the right place.

All documents shall be kept for at least the duration of the project or subsystem.

4.2 QA requirements for Assembly, Integration, and Tests (AIT)

4.2.1 Assembly, Integration, and Test control

Each subsystem shall foresee a detailed Assembly, Integration and Test (AIT) plan. The test plan shall state the type of the test, the test approach, the configuration of the assembly under test and the pass/fail criteria. A test report shall describe the obtained results.
An AIT/AIV responsible shall follow these processes assuring an updated version of the document.
For each test the AIT plan has to discuss in detail the following items:

- Test objectives
- Test description
- Test conditions
- Hardware and Software configuration
- Test pre-requirements
- Test equipment (including test software and equipment calibration)
- Required manpower
- Test responsible
- Hazards and safety precautions
- Acceptance/rejection criteria
- Cleanliness and environmental conditions of integration/test facility

Assembly, integration and test activities to be carried-out in the integration area shall be those described in the AIT plan and detailed implementation steps shall be provided into dedicated AIT procedures. In particular, test and/or inspection procedures shall give sufficient detail as to allow the results of repeated tests to be compared, and, also, to detect any trend towards out-of-specification conditions.
AIT activities shall be carried-out by dedicated teams of engineers, under the responsibility of the appointed AIV responsible, and an AIT/AIV Plan shall be issued. The PA responsible shall ensure a proper control, recording, and documentation of test data, and shall maintain an adequate non-conformance control system for the assembly level he/she is responsible for. He/she is also in charge of ensuring that the status of hardware is maintained and controlled during the AIT phases.
A step-by-step procedure including inspections shall be reviewed and approved prior the activities start.
Any end-item delivered to the AIT plant by suppliers and subcontractors and requested to be assembled or integrated at the higher level of assembly, shall undergo a formal incoming inspection by QA personnel, prior to be moved to the AIT area.
The PA responsible shall authorize the acceptance of the hardware for the use intended or, otherwise, shall state the necessary actions based on applicable TRB/DRB minute of meeting result held.
KIP and MIP will be identified in accordance with the following criteria:

- when critical processes are performed;
- when formal qualification and acceptance tests are foreseen;

- when the manufacturing sequence makes the item difficult and costly to disassemble for inspection;
- when the manufacturing sequence or renders the location inaccessible for inspection.

A MIP requires the participation of a SST representative or at least a written SST agreement to proceed. A KIP may be performed as scheduled if there is no reaction from SST.

Tests and assembly operations shall be reported in a logbook containing the most important data (applicable procedures, responsible of the operation, date, cleanliness, environment, etc.). This logbook shall be made available for verification to the SST-PRO.

4.2.2 Test facilities, equipment, and tools

Test facilities required to conduct the test programme shall be specified in the AIT plan.

The supplier shall ensure well in advance of testing that test facilities, equipment, and tools conform to specified requirements.

All test equipment including commercial test equipment will be calibrated as required prior to use and shall remain within calibration during use.

Prior to unpacking and test of the equipment, the test facility will have been set up in accordance with the applicable test procedure, and the facility cleared of all obstructions.

4.2.3 Test documentation

4.2.3.1 Test procedures

Test procedures will be produced for all tests contributing to qualification and acceptance on deliverable hardware and software. They shall be derived from the project or subsystem requirements of the AIT plan and shall completely and precisely define the methods and steps by which the tests will be carried out; acceptance criteria shall be clearly indicated.

The test procedures will include:

- applicable documents;
- identification of the product under test;
- test equipment and set-up;
- scope of the test, including the identification of the requirement being verified;
- test flow;
- step-by-step procedure, including definition of specific steps to be witnessed by QA personnel;
- data to be recorded and checked;
- pass/fail criteria and test data evaluation requirements (including test results tolerance when needed).

For each step the following items shall be reported:

- sequential ID number of the performed action
- summary description of the performed action
- name of parameter to be checked
- expected parameter value
- measured parameter value
- action result (PASSED/FAILED)
- additional notes

The supplier QA organization shall review and approve test procedures.

4.2.3.2 Test reports

The supplier shall ensure that all tests are comprehensively documented in test reports, and that they include, as a minimum:

- reference to the applicable test procedure, and description of the deviations from it during the actual testing;
- identification of the product under test;
- a list of the test equipment configuration and calibration status;
- a list of Non-Conformance Reports raised during the test;
- the as-run filled-in test procedure including initial configuration checks;
- all test data including environmental test facility records (i.e., temperature and humidity figures, during tests);
- clean room environmental control data (i.e., temperature, pressure and humidity, during qualification and acceptance tests);
- photos in case a visual inspection is part of the verification procedure;
- test data records and evaluation;
- a summary (evaluation and verification) of the test results and a conclusion.

The Project or subsystem QM shall review and approve test reports.

4.2.4 Test Witnessing

Critical development tests and formal qualification and acceptance tests will be monitored or witnessed by QA personnel to ensure that applicable procedures are followed without errors, and that records of the activities and test results are taken.

4.2.5 Test reviews

The supplier shall ensure that Test Readiness Reviews (TRRs), Post Test Reviews (PTRs), and Test Review Boards (TRBs) are performed, respectively, before, immediately after and at the end of the elaboration of the test results.

Before the execution of any test, the TRR shall verify:

- the conformance between the as-built configuration status of the test sample and the design baseline;
- status of non-conformances / failures, requests for waivers, requests for deviations and open work;
- the availability and the approval status of the test procedures;
- that hazards and hazardous operations have been clearly identified within the test procedure and appropriate actions are implemented;
- readiness of test facility and associated equipment (cleanliness of test facility, calibration status and validity of all test equipment, including any software programme);
- responsibilities during the test.

The supplier shall inform in advance the relevant PO of the test execution and invite a PO representative to attend it. The Project QM, in collaboration with the QA responsible for the external supplier, shall monitor that all the quality assurance activities are followed and, in particular, that:

- The approved procedures are applied during the test;
- No errors arise during the execution of the procedures;
- Record and logbook of the activities are taken;
- Non-conformances are traced following rules reported in Section 8.

After major portions of qualification and acceptance tests (e.g., at the end of EMC or vibration tests), a PTR shall be held to determine that:

- all portions and steps of the applicable procedure have been properly executed, and the test specimen and test equipment have been brought into a safe condition;

- all deviations from or modifications to the initial test procedure which had to be made during the test were properly authorised;
- all required data records are complete and at least a first assessment has been made to determine whether the parameters were within required limits, or whether there is a need for additional testing and/or further analysis of the results before a conclusion can be reached;
- non-conformances/failures have been recorded and at least initial dispositions affecting continuation/completion of the test have been made by the appropriate Material;
- conclusion, whether the test article can be released to the next step or the test set-up can be dismantled.

After the test and the analysis of recorded data has been concluded, a Test Review Board (TRB) shall be convened to:

- Ensure that all the procedure steps have been properly followed;
- Ensure that required data records are complete and parameters are within the requirements;
- Ensure that non-conformances and failures are traced;
- Ensure that deviations in executing procedures are authorized and traced;
- Review the analysis made of the test results;
- Confirm conformance to test requirement specification.

When analysis necessary for TRB are available at the time of the PTR, PTR and TRB can be combined.

The Programme QM, in collaboration with the Project QM and the QA responsible of the external supplier (if any), shall be represented in the formal boards established for the TRBs.

At the end, the responsible of the test shall prepare a test report containing description of how the procedure has been executed, if authorized deviations are present, the test results and if it presents eventual failures and non-conformances.

4.3 QA guidelines for procurement

4.3.1 Selection of procurement sources

The internal and external suppliers (hereafter purchasers) are responsible not only for the quality of their own products but also for the quality of the products procured by them. The selection of manufacturers and suppliers shall be driven by proven ability in procurement of materials, parts, and components needed by the project or subsystem. They must guarantee their capability concerning the quality control and traceability. The demonstration of capabilities shall be based on the successful supply of items or services similar to those to be procured.

It is responsibility of each purchaser to define criteria for evaluating and selecting its suppliers from a quality point of view, and to apply this PA Plan also to its suppliers.

4.3.2 Quality Agreement with Suppliers

A quality agreement with the selected external suppliers should be included in all procurement contracts. The only exception is for commercial products off the shelf (COTS), for which documentation and configuration management will be subject to manufacturer definition.

The quality agreement establishes:

- The quality requirements applicable to the supplier.
- The need of a supplier’s quality plan and control plan.
- The tests, inspection and controls before, during and after production which the supplier has to implement.
- The list of special characteristics to be controlled by the supplier, including method and frequency.
- The calibration documentation, showing the status of test equipment used for controlling critical characteristics.

- The file format which should be used for exchanging technical drawings between the purchaser and the supplier.
- The warranty conditions.
- The procedure for solving non-conformances (see Section 8).
- The packaging requirements.
- The requirements for product identification, marking and labelling
- A signed Capability Commitment, where the supplier confirms to be capable of meeting all requirements and of supplying the requested quantity and quality on schedule.
- The documentation which the supplier shall attach to each delivery, for example:
  - As-built configuration with product number, revision index, production date and serial numbers of components and sub-components.
  - Test results, inspection logs.
  - Material certificates.
- Other supplier documentation: maintenance manual, spare parts lists, RAMS data, operation manuals, transport and handling instructions.

4.3.3 SST contracts

Each SST contract shall include a Statement-of-Work (SoW) and Applicable and Reference documents.
The SST contracts shall include all the technical requirements applicable to the purchasing contract.
This PA Plan is an applicable document for all the SST contracts. For the industrial partners, suppliers of lower-level parts/components, the applicable standards and requirements will be agreed case by case (in the SoW or within a specific document, if/as deemed appropriate) for all the activities under their responsibilities.

4.3.4 Record and list of procurement sources

The QA responsible of the purchaser shall establish and maintain records of the procurement sources.
The industrial partners shall submit to the Programme QM, upon request, the list of procurement sources.

4.3.5 Surveillance of procurement sources

The purchaser shall exercise surveillance over all the activities carried out by its suppliers.
The surveillance programme shall address audits, reviews, mandatory inspection points, as well as direct supervision at the suppliers' facilities and source inspection. An example of review is the Critical Design Review (CDR).
The purpose of supplier surveillance is to ensure that PA Requirements are met by the suppliers during design, procurement, manufacturing, assembly, and test phases. The PA/QA responsible shall be in charge of supplier survey and shall have direct contact with the supplier's PA managers.
The aim of audits is to evaluate operations, activities, facilities, equipment, personnel and procedures to assess performance effectiveness, identify potential deficiencies, provide feed-back to management, and ensure implementation of timely corrective actions.
The PA responsible shall perform periodical audits/inspections at the sites to detect actual or potential deviations, system incompatibilities and anomalous conditions with respect to applicable Plans and in accordance with frequency and modalities defined at project or subsystem level.
The performance of the subcontractors will be monitored at all Progress Meetings. In case of specific problems, dedicated meetings will be arranged. Subcontractors are also requested to provide monthly regular Progress Reports (which may be included in the Project Progress Report) according to the following layout:

- Project Name

- Status of on-going activities: this section shall contain information about the status of the SW and HW development activities, e.g., documents produced (deliverable or internal), documents baseline, review performed, current life cycle phase.
- Performed Activities: this section shall give the list of the activities performed together with general assessment of the results of the activity (e.g., quality of the product inspected).
- Deliverables: this section shall define the list of the deliverable documentation produced by the subcontractor organization.
- Major problems and proposed solutions: this section shall describe problems encountered during the performing activities at subcontractor level, along with proposed solutions and general recommendations.
- Open Items: this section shall define the status of all open items as listed below:
  - Status of RIDs or general formal comments;
  - Status of Action Items;
  - Status of problems identified in internal Audit or inspections;
  - Status of SW-HW Non-Conformances (NCRs);
- Overview of the risks identified by the supplier
- Planned Activities: this section shall contain a list of planned activities for the next report period.

A formal non-conformance reporting and close out system shall be imposed on each subcontractor, to ensure that problem areas are correctly disposed and followed up.

Surveillance activities will be scheduled and managed taking into account the overall Project schedule.

4.3.6 Documentation for Procurement

All the documentation related to procurements shall follow PA rules and shall report the requirements for quality control, the traceability and the appropriate standard. Conformance documentation shall be requested and act as an entry point into the manufacturer’s traceability system.

It is responsibility of the QA responsible to verify that all inspections, tests, and witnessing of critical processes are performed and that the necessary documentation is provided.

The documentation related to quality that the supplier shall prepare is:

- Production layout and process flow diagram
- Process FMEA
- Control plan (and control charts if applicable)
- Process capability study (if necessary, only for special products: high amount, high complexity, schedule relevant)
- Check lists for incoming inspection
- Check lists for final inspection before delivery
- Material certificates
- Certificate of conformance
- As-Built Configuration List
- As-Designed Configuration List
- Detailed Assembly Drawings and Part Lists
- Test plan for checking the packaging of products that require special transportation conditions
- Non-Conformance Reports
- Requests for deviation/waiver (if a non-conforming product needs to be delivered)
- Acceptance Test Report, including test data sheets with acceptance signature;
- Documentation Status list (if necessary)
- Packing List.

The documentation related to quality assurance in the procurement process that the purchaser shall prepare is the following one:

- Quality agreement with suppliers
- Audit of suppliers (audit questionnaire and audit report)

The traceability system of the procured items is based on log books. Operations logged are:

- Manufacturing (manufacturing record)
- Tests and Inspections
- Integration
- If the case, non-conformance detection

5 QA requirements for delivery and acceptance

The content of this section applies to both internal and external suppliers of the SST Projects, and regards both hardware and software items.

5.1 Acceptance process

The planned delivery and acceptance reviews at system level are defined in the SST PMP [AD1].
Each SST Project shall agree and apply with each of its industrial partners or suppliers a formal acceptance process for all deliverable items, at any contractual level, to ensure that conformance of the items to be delivered is fully assessed and documented. It shall include at least a subsystem Acceptance and Delivery Review (S-ADR). The S-ADR shall verify that the deliverable subsystem is compliant with the requirements reported in the contractual SoW.

5.2 Acceptance Data Package

The supplier shall provide an Acceptance Data Package (ADP) for each deliverable item. The ADP shall contain a complete history of the deliverable item, with all documents regarding the deliverable item (as listed in Sections 4.1.7 and 4.3.6) and any certification required by either the program or local safety laws.
The ADP shall include:

- Title page;
- Table of Contents;
- Change log;
- Certificate of Conformance (CoC);
- Cleanliness certificate (when applicable);
- Critical Item List;
- Safety assessment;
- List of all Problem Reports and NCRs and copies of major ones;
- List and copies of all Request for Waivers/Deviations (RFW/D);
- Copy of the full “As-Designed/As-Built” Configuration Item Data List (CIDL);
- Drawing Delivery Package;
- Interface documents / User Manual / Operation and Maintenance Manuals;
- Overall Test Flow Chart and copies of all MIP/KIP reports;
- Test Reports, including as-run procedures;
- Verification Control Document;
- Historical Record Sheets ("logbook");
- Installation Procedures (including alignment, calibration, etc.);
- Packaging, Storing, Transport and Handling procedures;
- DRB minutes (in the final ADP after DRB).

The ADP shall include also a ‘Summary Report’ of the overall test campaign performed. This Summary shall provide:

- the list of the performed tests
- the list of the produced NCRs
- an overall evaluation of the test results
- a declaration about the item compliance to applicable specifications

This Summary Report shall be considered as the ‘Identity Card’ of the tested item, which shall be associated to the item itself during all its operational life.

Handling, cleaning, packaging, marking, labelling, storing and transport procedures will be part of the ADP.
The ADP shall include also the list of ADPs and logbooks of units and subsystem supplied by lower-tier supplier.
The QM shall check completeness and consistency of the ADP as defined in the contractual documents and constituted by the configuration responsible.
In case of equipment storage or return back to supplier, the initial individual log sheet shall be fulfilled with complete description of all events in the life of the hardware starting from incoming inspection.
The ADP shall constitute the basis for formal acceptance reviews.
The ADPs shall be maintained and integrated into higher level ADPs during subsystem or system integration and testing.

5.3 Delivery review board

Upon completion of the test sequence and final inspection, a formal acceptance of deliverable items shall be performed.
A Delivery Review Board (DRB), as contractually required, shall be convened to review all relevant data, to prove that all specified requirements have been satisfied and that any deviations/waivers are properly documented and accepted, and, finally, to authorise the item for delivery.
The supplier shall ensure that a Delivery Review Board (DRB) is convened prior to the delivery of any item to SST (in case of the DR) or to CTAO (in case of the PAR and of the FAR).
The DRB shall be composed, at least, of the following members:

1) Representatives of the SST PO:
    a) Project manager, or authorized representative, as chairman;
    b) PA manager, or authorized representative;
    c) System Engineer, or authorized representative.
    d) WP leader
    e) AIV Manager
2) Submitting supplier’s representatives:
    a) Project manager, or authorized representative;
    b) PA manager, or authorized representative;
    c) System Engineer, or authorized representative.

The DRB shall:

1. Confirm list of deliverable items;
2. Review the Baseline Configuration (as-designed), including relevant change proposals and reconciliation of changes;
3. Review the actual build status for hardware and software (as-built):
   a. Review the status of non-conformance (major + minor).
   b. Review the status of waivers/deviations.
6. Evaluate inspection results including cleanliness status
7. Verify witness samples
8. Verify MIP/KIP reports
9. Review the status of the test programme/test flow and test reports
10. Review the verification status of requirements in the Verification Control Document (VCD)
11. Review Qualification/Acceptance test successfully run
12. Evaluate Operational constraints, Operating and Maintenance Manuals.
13. Review the hardware status and procedure of packaging, handling shipping, and storage operations.
14. Perform visual inspection of HW.

15. Authorise shipment.

The DRB shall be responsible for authorising the delivery of the items under acceptance, and certifying in writing that:

1) the items conform to the contractual requirements and to an approved design configuration;
2) the items are free from material and workmanship deficiencies;
3) all non-conformances are closed-out, or corresponding plans, compatible with the delivery, are accepted;
4) the relevant ADP is complete and accurate.

Delivery shall only be authorized by the unanimous agreement of the DRB members.

If the review is declared positive, the product is accepted and it is certified to be compliant with the applicable requisites and guidelines.

For the acceptance a certificate of conformance shall be made available and signed by the supplier.

6 Quality Assurance programme for Hardware

The content of this section is applicable to both the internal and external suppliers of the SST Programme. It describes the Quality Assurance programme specific for hardware items, which include mechanical, electrical, electronic, and electromechanical items.

6.1 Product Identification

Product identification is fundamental for proper control of the system configuration and for future maintenance activities and product upgrades. All parts and components produced or purchased shall be clearly identified with a configuration item number and a serial number **Error! Reference source not found.**. This information shall be engraved or placed in such a way that it cannot be removed or deleted accidentally. At each delivery the identification data of the delivered items shall be recorded and stored in a proper document. For electronic components with firmware, there shall be the possibility to know the firmware used version by means of a specific command. The firmware should be password protected in order to avoid accidental or unauthorised changes.

6.2 Traceability

The supplier shall be capable to trace data, personnel and equipment related to procurement, manufacturing, inspection, test, assembly, integration, and operations activities.
The supplier shall be capable to trace backward the locations of materials, parts, sub-assemblies, and to trace forward the locations of materials from raw stock.
Each part, material or product will be identified by a unique and permanent part or type number. To assure a full traceability capability the following rules will be followed:

1) identification numbers are assigned in a systematic manner,
2) identification numbers of scrapped or destroyed items are not used again,
3) identification numbers, once allocated, are not changed, unless the change is authorized by the customer.

A logbook will be prepared and maintained, at system, subsystem, and assembly level, for all operations and tests performed on the developed items. The logbooks will contain historical and quality data and information which is significant for operation of the item, including non-conformances, deviations, and open tasks.

The Logbook template reference is the following:

- References/General information on the product;
- Contents;
- Approvals of the relevant authorities (QA, PA, PM);
- Customer acceptance (if required by the business agreement);
- Hardware configuration and traceability table, which reports all the identification references of single elements composing the CI;
- Hardware configuration change and status table, which reports for each single element of the CI all the events relevant to integration, removal and replacement on the higher level;
- Summary list of the integration and test instructions, including for each entry, the action start date, action performed date and action close–out date (for example shop travellers);
- Summary list of non-conformances with relevant identification references, issue date, closure dates, and status;
- Records of total operating hours for each limited–life element identified in the test procedures;

- In chronological order, the events related to the integration and test activities performed on the relevant item (i.e., system, subsystem, and equipment).

6.3 Metrology and calibration

The supplier shall control, calibrate, and maintain inspection, measuring, and test equipment at prescribed intervals, or prior to use.
The supplier shall maintain calibration records for inspection, measuring, and test equipment, and shall make them available to the Programme QM upon request.
The supplier shall use equipment in a manner which ensures that measurement uncertainty is known and is consistent with the specified measurement capability.
The supplier shall include in the calculations of all measurements the total error in the measurement process attributable to the cumulative error from the calibration chain, measuring equipment, and those contributed by personnel, procedures, and the environment.
The supplier shall select inspection, measuring, and test equipment in conformance with the required measurement accuracy and precision.
The supplier shall establish, document, and maintain calibration procedures, including details of equipment type, identification number, location, frequency of checks, check method, acceptance criteria, and the action to be taken when results exceed the specified accuracy.
The supplier shall ensure that the environmental conditions are suitable for the calibrations, inspections, measurements, and tests being carried out.

6.4 Handling, storage, and preservation

Quality Assurance personnel will verify that manufacturing, assembly, integration and test documents contain relevant handling procedures and instructions to guarantee integrity of the items.
Special boxes, containers and transportation vehicles shall be utilized for items which are susceptible to handling damage. Special handling equipment and controlled areas shall be provided for proper handling of critical items.
The supplier shall place in secure storage areas incoming materials, intermediate items needing temporary storage, and end items before shipping. These areas shall guarantee the storage conditions applicable to the involved items. Each storage area shall be identified and labelled for its intended use.
The supplier shall maintain control over acceptance into and withdrawal from storage areas.
The supplier shall maintain records to ensure that all stored items are within the usable life limits, controlled and retested, and to provide traceability within the storage or segregated area.
The supplier shall maintain records of the expiry dates of those materials and chemicals used in production that need to be strictly observed.
Adequate safety and cleanliness, preventive maintenance and age control shall be provided. Limited life items shall be specially identified and controlled with respect to shelf life time.
Preservation against deterioration, damage, corrosion, contamination or possible confusion of items shall be accomplished to protect hardware during operations, transport and storage.
It shall be also checked that preservation instructions, including material and process definition, are contained in the manufacturing documents and are accomplished.
After cleaning, the parts or materials shall be carefully dried and subjected to a visual examination, to ensure that the surfaces are free from dust, oil, grease or corrosion.

6.5 Material Certificate

A material certificate proves that the quality and properties of the material correspond to the specifications and standards provided by SST [SD1-SD23]. It can either just confirm the compliance with an international norm or it can contain the results of a chemical analysis and/or physical test made by a certified laboratory together with a statement that the required specifications are met. All electrical items shall be CE marked.

The suppliers should be requested to attach a material certificate to each delivered batch of critical or relevant parts (for example for the steel of the telescope structure, special fixation screws, concrete of telescope foundations, etc.). The supplier should have, and forward to the quality representative of the purchaser if requested, a copy of the material certificate corresponding to raw material it used for the produced parts.

6.6 Receiving inspection

6.6.1 Receiving inspection planning

In case of incoming items, the Project or subsystem QM shall perform inspections of all incoming supplies in accordance with established procedures and instructions, to ensure that quality level is properly determined. He/she shall ensure that all incoming supplies, including documentation and packaging, whether delivered on his/her own premises or elsewhere, conform to the requirements of the procurement documents.

The QM shall create an incoming inspection check list describing how to carry out the inspection, the characteristics to be controlled, the sampling frequency, the pass/fail criteria, the necessary tools, the person who carries out the inspection, and how to proceed when the product shows a non-conformance (see Section 8). The checklist should be filled in for each incoming inspection and forwarded to the head of production for revision and acceptance of the batch or the product before storing it in the warehouse or bringing it to the production line. The data of each incoming inspection is part of the quality records and shall be kept until the final decommissioning of the observatory for traceability purposes. When the number of pieces is high and an incoming inspection of all parts is not feasible, the quality representative may choose a sampling method.

Receiving inspectors shall have available the procurement documents, specifications, drawings and any other document relevant to incoming supplies as required in the procurement documents.

6.6.2 Receiving inspection activities

Receiving inspection activities shall include:

- verification that the packaging meets the requirements and is not damaged
- verification that the environmental sensors and the shock and tilt indicators (if any) are not damaged
- visual inspection of the delivered items, in order to assess that product looks OK at a first glance (no loose parts, dents, cracks, etc.)
- verification that the product corresponds to the type, model and characteristics that had been ordered
- verification of correct identification and, where appropriate, configuration identification for conformance to the ordering data,
- verification that the quantity of pieces, batch number and serial numbers match with the packing list and with the purchase order.
- verification that the required documentation is attached to the delivery (packing list, as-built configuration, level of engineering, handling and safety instructions, conformance certifications, documentation on tests, etc.).
- identification of the inspection status and physical separation of the supplies in the receiving inspection area according to the following categories:
  (a) items for which the receiving inspection has not been completed;

(b) conforming items;
(c) non-conforming items.

- prevention of unauthorized use of uninspected and non-conforming items,
- identification of the items to be released for production with conformance status and traceability data to be recorded in manufacturing documents

In case any of the inspected parameters shows a non-conformance, the entire batch shall be put immediately in quarantine and clearly labelled to prevent that it arrives to the assembly/production line (see Section 8). The next step is to launch a non-conformance report describing the problem and to inform the responsible of the involved WP, in order to decide if the batch can be accepted after a full inspection of all parts, can be reworked, or if it must be rejected and sent back to the supplier (see Section 8).

6.6.3 Receiving inspection records

The Project QM or, in case of an external supplier, the supplier QA responsible shall maintain receiving inspection records to ensure the traceability and the availability of historical data, to monitor supplier performance and quality trends.

6.7 Qualification testing

The QA responsible shall verify that all configuration items and their constituent items, either off-the-shelf or specifically designed, are properly qualified with margins respect to the SST application and environmental conditions. The status of each equipment shall be verified by reviewing previous qualification report data collected into the relevant End Item Data Package.

To obtain authorization to initiate qualification tests, the supplier shall demonstrate that:

1) the qualification model is fully representative of the deliverable item and all differences have been analysed to evaluate their effect on the qualification status
2) inspection and test requirements are expressed in an unambiguous and quantified manner, including: test procedure; test conditions; test standards (if any); applicable test levels, durations and tolerances; accuracy in measurement
3) the qualification test procedures and facilities are defined and available

The applied test procedure shall state the type of the test, the test approach, the configuration of the assembly under test and the pass/fail criteria.

A test report shall describe the obtained results.

6.8 Product manufacturing

During the production phase of the HW items the goal of the quality activities is to deliver products that are free of defects. For achieving this, it is necessary to procure defect-free raw materials and components, to have stable production processes, adequate controls along the production chain and trained personnel for operating the processes.

A production layout, work flow and manufacturing Process Failure Mode Effects Analysis (PFMEA) should be created before the beginning of the production phase. This allows the definition of the controls that are necessary at each step of the production and to document them in form of control plans.

Manufacturing Flow Charts (MFC) will be prepared to indicate all operations during manufacturing and equipment-level assembly in sequence. These flow charts will also identify key and Mandatory Inspection Points.

Items manufactured or assembled by internal and external suppliers shall be subject to QA control including inspections and test programs in order to ensure that the completed article is compliant with applicable drawing, specification and procedure requirements and to ensure that production activities do not degrade the quality designed into the product.

6.8.1 Identification of Special Characteristics

Special characteristics are particularly important product characteristics or process parameters which require additional measures in order to assure their compliance. They can affect fit, form, function, performance, subsequent processing, safety or compliance with government regulations.

The product suppliers and the QA representative shall identify, define, and document the special characteristics of the product and of the production process, based on the design FMEA and PFMEA analysis. Special characteristics should be clearly identified in the technical drawings, the control plan, and the work instructions.

A waiver or deviation cannot be requested for a special characteristic that departs from the required value. Products whose special characteristics are nonconforming should never be approved nor delivered to SST.

6.8.2 Planning of manufacturing, assembly and integration activities and associated documents

The product supplier shall document the planning of manufacturing, assembly and integration operations and of inspections in the manufacturing plan or flow chart for the product, including the sequence of operations and associated inspections and tests. All steps reported in the manufacturing flow chart shall be described and numbered.

The planning shall include the reference to the procedures by which the various activities are performed and (if necessary) the required cleanliness levels and temperature and humidity requirements of the facilities.

The supplier shall issue and maintain manufacturing, assembly, and integration documents in accordance with established and released procedures.

The QA organization of the supplier shall review and approve such documents, and any modifications thereof.

The supplier shall provide detailed support documents and instructions, such as drawings, procedure and instruction sheets, to enable operations to be correctly performed.

6.8.3 Control of processes

The supplier shall monitor all processes used for manufacturing, assembly and integration, and enforce all applicable process requirements.

The supplier shall ensure that all manufacturing processes are covered by documented process specifications or standards.

The supplier shall describe in a specific document the procedure adopted to perform the process control.

Control plans shall be kept updated and shall be audited by the quality representative/officer.

6.8.4 Special processes

The supplier shall establish and implement procedures and controls for special processes, to ensure that:

1) Special processes are validated for the intended application.
2) Personnel who perform or inspect special processes are trained and certified
3) Materials, equipment, computer systems and software, and procedures involved in the performance of the special process are validated and monitored.

6.8.5 Process FMEA (PFMEA)

The supplier shall prepare a Process FMEA (PFMEA) which analyses the steps of the production process, in order to identify and evaluate the potential failures that can occur and prioritise the action items for alleviating the risk. The PFMEA shall undergo as many analysis loops as necessary until the risks are solved or minimized by means of a re-design of the production process and additional controls and error-proof methods.

6.8.6 Preparation of the Control Plan

A control plan shall be prepared, according to the production flow and FMEAs results.

The need of a control plan should be included as a requirement and the quality representative of the customer should check that the supplier has implemented it properly.

The control plan should include the following sections:

1) Information Table, which includes information of the part number, drawing number, supplier or contributor, contact information, approval dates, etc.
2) Process, which reports the list of those production steps in which a control or inspection activity takes place, together with the equipment, tool or machine needed to complete the step itself
3) Quality Characteristics of Product and Process, which reports the identifying number and the description of the characteristic being inspected or controlled
4) Control Methods, which reports:
    a) the specification and tolerance for each characteristic;
    b) the measurement method to collect the data;
    c) the sampling plan;
    d) the responsible in charge of making the controls;
    e) the reference number to a reaction plan flow-chart, that tells what to do in the event of an out-of-control or out-of-specification condition.

6.8.7 Critical Design Reviews

Before starting production of the first deliverable item, a Critical Design Review (CDR) at system level should take place for making sure that the criticalities have been solved, the inspections and control plans are in place and the production process is capable of producing the required quality and quantity on schedule. As stated by the SST PMP [AD1], this review shall be organized and conducted jointly by the SST Programme and CTAO, with CTAO acting as decision-making authority.

This system CDR shall evaluate the following aspects:

1) status of system definition and requirements, differences with the status of the qualification model, and impacts of these differences;
2) status of assembly, inspection and test documentation, differences with the status of the qualification model, and impacts of these differences;
3) implementation status of dispositions for risk reduction, as defined by risk assessment, into the assembly, integration, inspection and test procedures;

The CDR Board will include representatives of PA, design and manufacturing.

If deemed necessary, the system CDR will be preceded by internal subsystem CDRs (S-CDRs) as appropriate. S-CDRs may take place if a given subsystem requires more detailed, internal, review than can be offered by an overall CTAO review prior to series production. This may be most appropriate for subsystems under industrial contract, such as SST-OPT and SST-MEC. These S-CDRs shall be internal to the single SST Projects or subsystems, without any involvement of CTAO.

These S-CDRs shall evaluate the following aspects:

1) status of subsystem definition and requirements, differences with the status of the qualification model, and impacts of these differences;

2) status of manufacturing, assembly, inspection and test documentation, differences with the status of the qualification model, and impacts of these differences;
3) status of manufacturing processes;
4) implementation status of dispositions for risk reduction, as defined by risk assessment, into the manufacturing, assembly, integration, inspection and test procedures;
5) availability of personnel and of specified materials and parts, production, measuring and inspection equipment, and calibration status, when relevant;
6) cleanliness of facilities, with respect to the specified cleanliness levels;
7) facility temperature and humidity with respect to requirements.

6.8.8 Workmanship standards

The supplier shall employ workmanship standards throughout all phases of manufacturing, assembly and integration, to ensure acceptable and consistent workmanship quality levels.
Workmanship standards shall identify acceptance or rejection criteria.
Tools shall be checked for accuracy during the production life at adequate intervals.

6.8.9 Cleanliness and contamination control

6.8.9.1 Cleanliness control

The supplier shall establish controls for cleanliness of manufacturing, integration, and test facilities, and the limitation of sources of contamination.

6.8.9.2 Cleanliness levels

Contamination-sensitive items shall be cleaned, controlled and maintained to the required cleanliness levels.
The required cleanliness levels for the deliverable items shall be indicated on drawings, specifications, procedures, or other documents controlling the manufacture, assembly, integration and test of the items.

6.8.9.3 Cleaning materials and methods

The supplier shall develop detailed methods for attaining the cleanliness levels specified for the hardware.

6.8.9.4 Contamination control

Contamination shall be minimized by operating in clean working areas and by proper handling, preservation, packaging and storage.
Contamination-sensitive items fabricated or processed in contamination-controlled environments shall be inspected, tested, modified or repaired in identical or cleaner environments, unless specific precautions are taken to protect the items concerned from contamination.

6.8.9.5 Cleanliness of facilities

Fabrication, assembly and integration of contamination-sensitive items shall be conducted in facilities that provide cleanliness levels compatible with the specified product cleanliness.

6.8.10 Manufacturing inspections

Inspections and tests shall be planned at the points of the manufacturing, assembly and integration flow where maximum assurance for correct processing and prevention of unrecoverable or costly non-conformances can be obtained.

Among the inspections and tests as part of the manufacturing, assembly and integration flow, Mandatory Inspection Points (MIPs) shall be planned and performed with participation of SST representatives.

MIPs shall be agreed with the SST PO on the basis of a list prepared by the supplier.

MIPs shall be selected in accordance with the criteria as defined below, when one or more of the following conditions apply:

- When maximum visibility of quality is given.
- When critical processes are performed.
- Where the next step of the manufacturing sequence:
  a) is irreversible, or
  b) makes the item difficult and costly to disassemble for inspection, or
  c) renders the location inaccessible for inspection.
- When the item, once installed in the next higher assembly, damages by its failure the higher assembly.
- When a potential adverse impact on the properties and integrity of the end product could occur, owing to the criticality or complexity of the manufacturing step.

A MIP shall require an invitation with the agreed notice before the event, and the participation of the SST representatives, or their written agreement to proceed without their participation.

MIP information shall include as a minimum:

1) Purpose and subject of the inspections,
2) Criteria for the selection,
3) Notification period,
4) MIP identifier,
5) MIP description,
6) Reference of procedures necessary to perform the MIP,
7) MIP location in the manufacturing and inspection flow chart or the AIV flow chart.

6.8.11 Logbooks

The supplier shall prepare and maintain system, subsystem and equipment logbooks for all operations and tests performed on the item.

The logbooks shall be made available to the Project QM upon request.

6.8.12 Manufacturing, assembly and integration records

The supplier shall establish and maintain manufacturing, assembly and integration records to provide all manufacturing, assembly, integration and inspection data required for traceability.

The documentation related to quality that should be prepared for the HW production includes:

- Production layout and process flow diagram
- Process FMEA
- Control plan (and control charts if applicable)
- Process capability study in specific cases (high amount, high complexity, tight schedule)
- Checklists for incoming inspections
- Test plan for checking the packaging of very delicate products
- Possible request of deviation/waiver

The records shall be made available to the Project QM upon request.

6.9 Preparation for delivery

6.9.1 Packaging

The supplier shall ensure that packaging materials, methods, procedures, and instructions are adequate for protection of items while at the supplier’s plant, during transportation, and after their arrival at destination. To this aim, quality representative of the subsystem will prepare a specific test plan for verifying that the packaging of especially delicate parts is adequate for the transport conditions. For critical and costly products, packaged items shall be protected against shocks, dust, water, and temperature gradients. Therefore, the use of shock and tilt indicators as well as humidity and temperature sensors could be taken into consideration, especially when a verification of the integrity of the product upon arrival to the site is technically not feasible or very complex. In such cases, it is necessary to define a threshold of humidity, temperature or shocks/accelerations and to design an appropriate packaging. Items (for example electronic components) which can be damaged by condensed water that may appear inside the packaging during transport due to large temperature and pressure changes should be protected additionally (with humidity absorbers, waterproof sealing, etc.). In case of procured products which are shipped directly to the installation site, the quality representative should inform the supplier about the transport and environmental conditions and should supervise that the packaging requirements are met. The packaging design should be tested by the product developers and approved by the WP manager.

6.9.2 Marking and labelling

The supplier shall ensure that appropriate marking and labelling for packaging, storage, transportation and shipping of items are performed in accordance with the applicable specifications.

6.10 Delivery

6.10.1 Shipping control

The supplier shall ensure that the items to be shipped from its plant are inspected before release and found to be complete, adequately preserved and packaged, correctly marked and accompanied by all the required documentation.

Accompanying documentation shall include the ADP and, attached to the outside of the shipping container, the handling and packing or unpacking procedure and any relevant safety procedure.

6.10.2 Transportation

The supplier shall make provisions for the prevention of damages to items during transportation.

If necessary, transportation boxes shall be equipped with shock and temperature indicators.

6.11 Installation, maintenance and decommissioning

Installation, maintenance and decommissioning have to be properly analysed and documented. An installation, maintenance, and decommissioning manual shall be released as part of the project or subsystem documentation.

7 Quality Program for Software

The objective of software quality procedures is to provide adequate confidence that all the SST developed or procured / reused software, satisfies the quality requirements throughout the product lifetime. In particular, that the software design, controls, methods, and techniques result in a satisfactory level of quality in the delivered product.

This requires the measurement and control of the quality of:

- development processes (software quality assurance)
- products (software quality control).

To this aim, the Software Development Team (WT5) shall prepare, maintain, and apply a specific Software Product Assurance Plan (SPAP). It defines the software quality and product assurance requirements to be applied for the design, production, testing, delivery, and operations of all the software products for the SST programme (from the high-level application software down to the firmware level). It is based on the principles of the standard ECSS-Q-ST-80C [RD 1]. This PA Plan shall be an applicable document for the SPAP.

7.1 Software Product Assurance Implementation

According to the SST PMP [AD1], the SST Working Team 5 (WT5) will be in charge for the design and development of the SST SW. It shall clearly define the scope of the software product and the internal organisation, identifying roles, tasks and responsibilities of the WT structure. The following topics shall be addressed:

1) organizational structure;
2) interfaces, either external or internal, involved in the project;
3) independence of the software product assurance function;

The WT5 shall individuate in its organisation a software product assurance manager and the resources to be used to perform the software product assurance function.

7.2 Software Process Quality Assurance

The software process quality assurance looks at the process used to create the final software product. The scope is to ensure that the appropriate development plan for the specific product is followed, and the required software standards are applied. In particular, the WT5 shall identify the adopted mechanisms for planning, controlling, and reporting on product assurance, as well as the procedures for alerts, audits, non-conformances, and for resolving detected software problems. This activity shall be performed according to [SD24].

The WT5 shall identify the list of the documents where all other related processes are adequately documented. These include:

- software development plan;
- software verification and validation plan;
- test plan;

The plan documentation can be updated to reflect possible changes during the development and reviewed at the relevant milestones.

7.2.1 Software Dependability and Safety

Software components shall be object of the dependability and safety analyses in order to identify the severity of the associated possible failures. Based on the performed analyses, the software components criticality will be assigned, classifying them as:

Class A: Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in catastrophic consequences.

Class B: Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in critical consequences.

Class C: Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in major consequences.

Class D: Software that if not executed, or if not correctly executed, or whose anomalous behaviour can cause or contribute to a system failure resulting in minor or negligible consequences.

In order to assure the dependability and safety of the critical software components several measures can be applied:

- use of software design or methods that have performed successfully in a similar application;
- insertion of features for failure isolation and handling (software failure modes, effects and criticality analysis: SFMECA);
- defensive programming techniques, such as input verification and consistency checks;
- use of a safe subset of a programming language;
- >= 70 % code branch coverage at unit testing level;
- full inspection of source code;
- witnessed or independent testing;
- gathering and analysis of failure statistics;

Critical software shall be subject to regression testing after:

- any change of functionality of the underlying platform hardware (example: instruction set of a processor);
- any change of the tools that affect directly or indirectly the generation of the executable code.

7.2.2 Software documentation and configuration management

Software configuration control will be performed, assuring traceability of the developed software configuration items, until final acceptance and utilization. Configuration items and included configuration elements shall be identified in order to cover all delivered products (including documentation). The Programme QM shall verify that the Configuration management system defined in the PMP [AD1] is used. Procedures for controlling the changes, delivering, marking, protecting and archiving the product shall be defined or referenced.

The WT5 is responsible, supported by the Configuration Control manager, of all the software configuration control activities:

- Configuration Identification: each configured software item shall be uniquely identified.
- Configuration Status Accounting: software change status recording, software releases.
- Configuration Management of documents.
- Configuration Management of source code.

Software problems shall be handled since the start of code unit tests, by reporting them following an appropriate procedure. Software Problem reports shall be issued and maintained in a dedicated database. Methods and tools to protect the supplied software, checksum type key calculation for the delivered operational software, and labelling method for the delivered media shall be defined.

A protection mechanism shall be implemented to prevent unwanted modifications or damages to the released software product (source code, executable code, database, data, etc.). In this frame it shall be assured that software products are provided with an identification key “checksum”. The checksum value shall be provided in the Software Configuration Item Data List. SW PA responsible shall ensure that the checksum value is associated to the product before the release, and that it is verified at the reception of provided products. In case the protection mechanism is based on a supplier specific tool, the tool shall be agreed with the customer.

7.2.3 Process metrics

Metrics shall be used to manage the development and to assess the quality of the development processes. The following basic process metrics shall be used by the WT5:

- duration (how phases and tasks are being completed versus the planned schedule);
- effort (how much effort is consumed by the various phases and tasks compared to the plan).

Process metrics shall be used by the WT5 and reported to SST-PRO, including: number of problems detected during verification; number of problems detected during integration and validation testing and use.

7.2.4 Design

Specific objectives will be defined to be considered for design properties, as completeness, consistency, modularity, robustness, adaptability.

Traceability from Software requirements to Software design is established.

7.2.5 Coding

The tools to be used in implementing and checking conformance with coding standards described in this document shall be identified by the WT5 before coding activities start.

The SW coding shall be performed according to the CTAO Software Licensing Policy [SD26], the CTAO Software Programming Standards [SD27], and the CTAO System Control Standards [SD28].

The WT5 shall document this process for the specific software product.

7.2.6 Testing

Testing shall be performed in accordance with a strategy for each testing level (i.e. unit, integration, verification against the technical specifications, validation against the requirement baseline, acceptance), which includes:

- types of tests to be performed;
- the tests to be performed, in accordance with the plans and procedures;
- the means and organizations to perform assurance function for testing and validation.

In case of retesting, all test-related documentation (test procedures, data and reports) shall be updated accordingly. This activity should be carried out in case a major change in the software.

The WT5 shall document this process for the specific software product.

Before starting the testing activities, the SW PA shall review the Test Plans and Test Procedures to ensure that the test procedures are adequate, implementable and traceable. Specifically, that:

- The test objectives identified in the plan are satisfied;
- The test typology is defined (functional, performance, etc.);
- For each test input, foreseen results and test execution conditions are defined;
- Each test procedure contains the step-by-step actions for performing the test;
- Automatically generated code (if any) has been correctly considered in achieving the project validation objectives

The software validation versus the Technical Specification and versus the Requirement Baseline shall be performed on an operational representative environment.

Before the start of any formal test campaign a Test Readiness Review (TRR) will be held, ensuring:

- The test configuration is as foreseen in the approved test documentation;
- The tests procedures and data are approved;
- Software verification matrix is established to demonstrate that each software requirement is covered by validation tests or verification;

- All tests are foreseen to be performed on the same software version without intermediate rebuild;
- Expected results are defined;
- Known Software Non-Conformance and Request for Waiver (RFW) are identified.

Following any formal test campaign, a Test Review Board (TRB) will be held ensuring that:

- test campaign is performed in accordance with the plan and procedures;
- tests execution is documented and traced;
- tests report is prepared and updated;
- test findings are analysed and actions for managing the SW remaining open NCRs are initiated;
- test documentation updating is foreseen to facilitate the subsequent maintenance phase.

The TRR/TRB at software level can be grouped with the TRR/TRB at equipment level.

The PA responsible at prime level will review the test documentation and will participate to the TRR and TRB as necessary to monitor that the subcontractor activities are compliant to the SW PA Requirements.

7.2.7 Product assurance planning for individual processes and activities

Here we report product assurance activities that are common for the WT5 in managing the software processes:

- verification of the correct implementation of the documentation configuration management
- verification of the conformance to the applicable procedures and standards
- verification of the application of the engineering measures to mitigate the risks associated with the critical software
- verification of the availability of development phases input documentation and tools
- verification of the metric evaluation process (metrication)

The software process assessment will be performed by the software product assurance by performing several activities or by verifying their performance as measured by the software engineers. Part of these activities is performed exploiting dedicated software tools and gives origin to product metrication object data. The results of the software product assurance activities performed shall be documented.

Software Requirements Analysis

The activities during the Software Requirements Analysis phase shall include:

- control of the completeness of the requirements list, to be sure it contains proper and sufficient inputs for deriving the software technical specification
- verification that the software technical specification includes, in addition to the functional requirements, all the necessary non-functional requirements
- verification of the completeness of the requirements traceability matrix

Software Architecture and Design

The activities during the Software Architectural Design phase (to be started only after the consolidation of the technical specification) shall include:

- verification of the availability of all the necessary design tools
- analysis of the software design, in order to verify that its complexity and modularity meet the quality requirements

The design evaluation will be performed in parallel with the design process, in order to provide feedback to the design activity:

- analysis of the software design documentation, in order to verify that it contains the appropriate level of information for maintenance activities

- verification of the completeness of the technical specification vs. software components traceability matrix

Coding

The activities during the software coding phase shall include the following code-related metrication in parallel with the coding activity, in order to provide feedback to the software developers:

- Cyclomatic complexity
- Nesting level
- Lines of code (LOC)
- Comment frequency
- Adherence to coding standard

Testing and Validation

The activities during the Software testing and validation phase shall include the following tasks:

- to verify the completeness of the test related documentation before the start of test activity
- to verify that the code is put under configuration control after successful unit testing
- to organise and perform internal Test Readiness Reviews (TRR) before validation activities
- to verify that test reports are adequately compiled and updated
- to verify the traceability between the test plan, requirements and the performed tests

Software Delivery and Acceptance

The SST software is not a standalone product, the software acceptance process will be part of the combined SST hardware/software acceptance activities. The activities to be carried out before the Software acceptance tests shall include the following tasks:

- to verify that the software validation against requirements is complete
- to verify that no major software problems are open
- to verify that the software to be installed at CTA SST site is generated from opportunely configured source code version

During delivery and acceptance test campaign any discovered problem will be documented in non-conformity reports.

7.3 Software Product Quality Assurance

The WT5 shall describe how metrication of the software product quality will be performed, to verify the implementation of the relevant quality requirements. Such metrication activity will give a figure of the product quality involving requirement, design, code, and testing activities as well as software documentation quality.

The WT5 shall describe how testing and validation activities will be performed, in accordance to the strategy defined for each testing level and adequately documented in related plans and procedures. In order to verify these activities, the Test documentation shall cover all the specific aspects, including the test environment, the hardware and software configuration, the exploited tools, and the possible test software necessary. Tests definition shall include the expected results and, in any case, the criteria for pass/fail determination.

Contingency steps for the failure case shall be specified. For the requirements not covered by a test activity, verification reports shall be produced documenting (or referring to) the verification activities performed. The defined set of metrics shall provide also a valid assessment tool to verify whether the test coverage goal has been reached.

All the software documentation produced during design, implementation, test, and verification phases shall be subject to SST configuration management, thus assuring the development and implementation traceability and permitting to maintain the software product during the operational phase.

7.4 Software Verification, Validation and Acceptance

Verification planning should result in specification of techniques such as traceability, milestone reviews, progress reviews, peer reviews, prototyping, simulation, and modeling.

Validation planning should result in specification of techniques such as testing, demonstration, analysis, and inspection.

Software validation and verification can be difficult to separate. We give here the definition usually adopted in the Systems Engineering world.

- Verification - verification tests: software process to confirm that adequate specifications and inputs exist for any activity, and that the outputs of the activities are correct and consistent with the specifications and input. These tests are performed by the development team. These tests cover the requirements identified within the specification document to show that expected functions are effectively performed by the resulting product. The items evaluated during the verification activities (reviews, unit testing, component testing, and acceptance testing process) are: plans, design documents, code, test cases.
- Validation - validation tests: software process to confirm that the functional requirements and performances are correctly and completely implemented in the final product. These tests are performed by the end-users (customer) of the software products. These tests are performed independently of the specification document and may highlight missing or mis-specified requirements. The item evaluated during the validation activities (demonstration feedback from users, acceptance testing, on-site usage during commissioning) is the actual product/software. These definitions consider that a software product can meet its requirements, but it may not satisfy the requirement in the eyes of the user.

7.4.1 Software Verification

The first step in the verification process is the verification of the requirement. Verification of requirements is a big part of delivering quality software. Most, but not all, software requirements are traceable to executable tests, but all requirements are verified using one or more of the five System Engineering verification methods listed here.

A requirement may need verification at more than one of the SW reviews. For example, a requirement may need verification for design and verification of functionality at the end when the code is complete. However, for most if not for all software the Testing Verification Method shall be used to verify the requirements

Therefore, any Software product that shall be delivered to the SST-PRO shall include software tests that demonstrate the code is well written and meets its requirements (unit tests, component tests and acceptance tests).

Use of automatic testing procedure is strongly encouraged. During Acceptance Testing the automated tests will be run along with any additional manual tests.

The WT5 shall produce a Verification Plan of the requirements. The plan maps at which SW review a requirement is verified and indicates the steps and Verification Procedures that will be used to verify the requirement. A Verification Report shall be produced to illustrate the results of the Verification Procedures.

Verification Method	Description	Activity
Design	Verification by Design is verification through review of design methods, design documentation, simulation models and/or design margins.	The software requirement is verified by review of documents.
Inspection	Inspection is verification by visual examination of the system or its components or verification by review of as-built system or system component documentation.	The software requirement can only be verified by inspecting the delivered software or delivered documentation.
Demonstration	Demonstration is verification by operation of the system or part of the system under a specific set of conditions to present observable behaviour showing compliance with the specification. Note that demonstration does not require the use of instrumentation, special equipment or subsequent data analysis.	The software requirement is verified by demonstrating the software capability to a stakeholder.
Test	Test is verification by operation of the system or part of the system, under predetermined appropriate conditions, using instrumentation or other special test equipment to collect data showing quantitative compliance with the specification.	This is the typical way of verifying requirements. Tests are constructed to show the proper operation and functionality of the software component. Tests are executed and used to verify functionality or performance.
Data Analysis	Data Analysis is verification through the processing of data accumulated from other verification methods, such as a series of tests, or a test that requires subsequent analysis of data to show compliance to a requirement.	The software requirement is verified through data analysis. An example might be performance data captured over several days or months.

Table 7-1: List of the verification methods for the SW requirements

7.4.2 Software Validation

Requirements flow to use cases and tasks that result in software deliverables, which are tested and can be demonstrated for the product stakeholder: SST users and operators and maintainers.

Software validation process consists of regular stakeholder involvement in each software iteration cycle, including regular demos and software validation reviews. Structuring the software as end-to-end features deliverable over the course of the software product implementation period allows continuous validation. It is expected that requirement validation (along with verification) will occur during commissioning and result in changes to the software and possibly new software requirements as users and engineers test the systems and get a better sense of how they are used.

8 Non-conformances

This Section describes the management of the non-conformances; it is applicable to both the internal and external suppliers of the SST Programme and regards both hardware and software items.

8.1 Definition

A non-conformance (NC) is an apparent or proven condition of any item, process, operation or service, in which one or more characteristics do not fulfil a specific requirement. It includes failures, anomalies, discrepancies, deficiencies, defects and malfunctions.

A NC may be detected in the product itself or in the process used for its realization. It can be detected in internal or external audits, tests, incoming inspections, during production, after production or even after the item delivery to the WP to whom it is intended.

Nonconforming items, processes, operations, service or documents for a system and associated equipment during design, procurement, manufacturing, assembly, integration, testing, and transportation activities shall be subjected to a NC control system that shall provide a clear approach for:

- identification and segregation of non-conforming items;
- recording, reporting, review, disposition and analysis of non-conformances;
- definition, implementation and verification of corrective and preventive actions.

8.2 Classification

NCs can be classified as MAJOR or MINOR.

A NC is classified as MAJOR if it affects the form, fit or function of a deliverable HW/SW item, or if it can have an impact on the following areas and cases:

- safety of people or equipment,
- operational, functional or any technical requirements
- reliability, maintainability, availability, lifetime
- functional or dimensional interchangeability
- changes to or deviations from approved qualification or acceptance test procedures
- approved HW/SW Interface Control Documents

A NC is classified as MINOR if, by definition, it cannot be classified as major, i.e. it does not affect the form, fit or function of a deliverable HW/SW item and have no impact on the items listed above. Examples of minor NCs are random failures, where no risk for a lot-related reliability or quality problem exists, and minor inconsistencies in the accompanying documentation.

8.3 Responsibilities related to non-conformances

It is the responsibility of any person involved in the project or subsystem who detects any service, process or product that does not meet the requirements, to report the problem immediately to the members of his/her WP and to the QM responsible for his/her WP.

In case the service, process or product affected by the detected non-conformance is provided by an external supplier, the relevant QM shall report the problem to the involved supplier.

It is the responsibility of the supplier (either internal or external) who provided the non-conforming item to ensure that the causes are investigated and solved in a satisfactory manner. The supplier nominates the Non-conformance Review Board (NRB), which shall be the sole technical authority for the treatment of non-conformances. In the case of internal suppliers, the NRB shall include the QM responsible for the involved WP, the WP manager/coordinator, and at least one representative for the

Engineering area. In the case of external suppliers, the responsible of the equivalent areas (PM, SE, PA) shall be involved.

8.4 Non-conformance reporting

Non-conformances shall be identified and recorded in a report (NCR), which has to be prepared and managed by the relevant QM and delivered to the SST PO for review. Each NCR shall be uniquely identified with a reference code, which shall be assigned according to the rules described in the SST Configuration and Data Management Plan [AD3]. The NCR shall report at least the following items:

- revision and date
- NC classification (major/minor)
- name or serial number of the NC item
- procedure or activity in execution when the NC is detected
- problem description
- originator of the reported problem
- test set-up
- environmental conditions at problem occurring
- configuration of the equipment under test (operating modes, connections, …)
- remedial actions adopted in order to proceed with the on-going activity
- preventive actions adopted in order to avoid the problem repetition on similar items
- corrective actions adopted in order to remover the causes(s) of the problem
- name and signature of person who has verified the effectiveness of the adopted solution

The template to be used for the NCRs of the SST Programme is reported in Appendix A.

Remedial/Corrective actions will be planned, initiated and carried out. In case no corrective actions are practicable, a request for deviation (RFD) or waiver (RFW) must be advanced.

Subcontractors will be requested to follow the same principles.

8.5 Procedure for handling non-conformances

For reporting and solving NCs, a non-conformance procedure shall be implemented. This non-conformance procedure shall be applicable to all approved parts, software, services, systems, subsystems and infrastructure of the SST Programme.

The process model reported in Figure 8-1 shows the steps for detecting, reporting, solving, and closing non-conformances detected by any supplier of the SST Programme. The reported procedure regards non-conforming items which can be either internally produced by the supplier itself or externally provided by a lower-tier supplier. It shows also the role and possible involvement of higher-level purchasers and customers and of SST.

The objective of this procedure is to respond to the unintended delivery of non-conforming products and to prevent undesired consequences. Furthermore, the causes of all non-conformances should be investigated and a Corrective Action Plan implemented, in order to avoid whenever possible a repetition of the same non-conformance.

This procedure should be mandatory for all suppliers (internal and external) and, then, it should be included as a requirement in all procurement contracts.

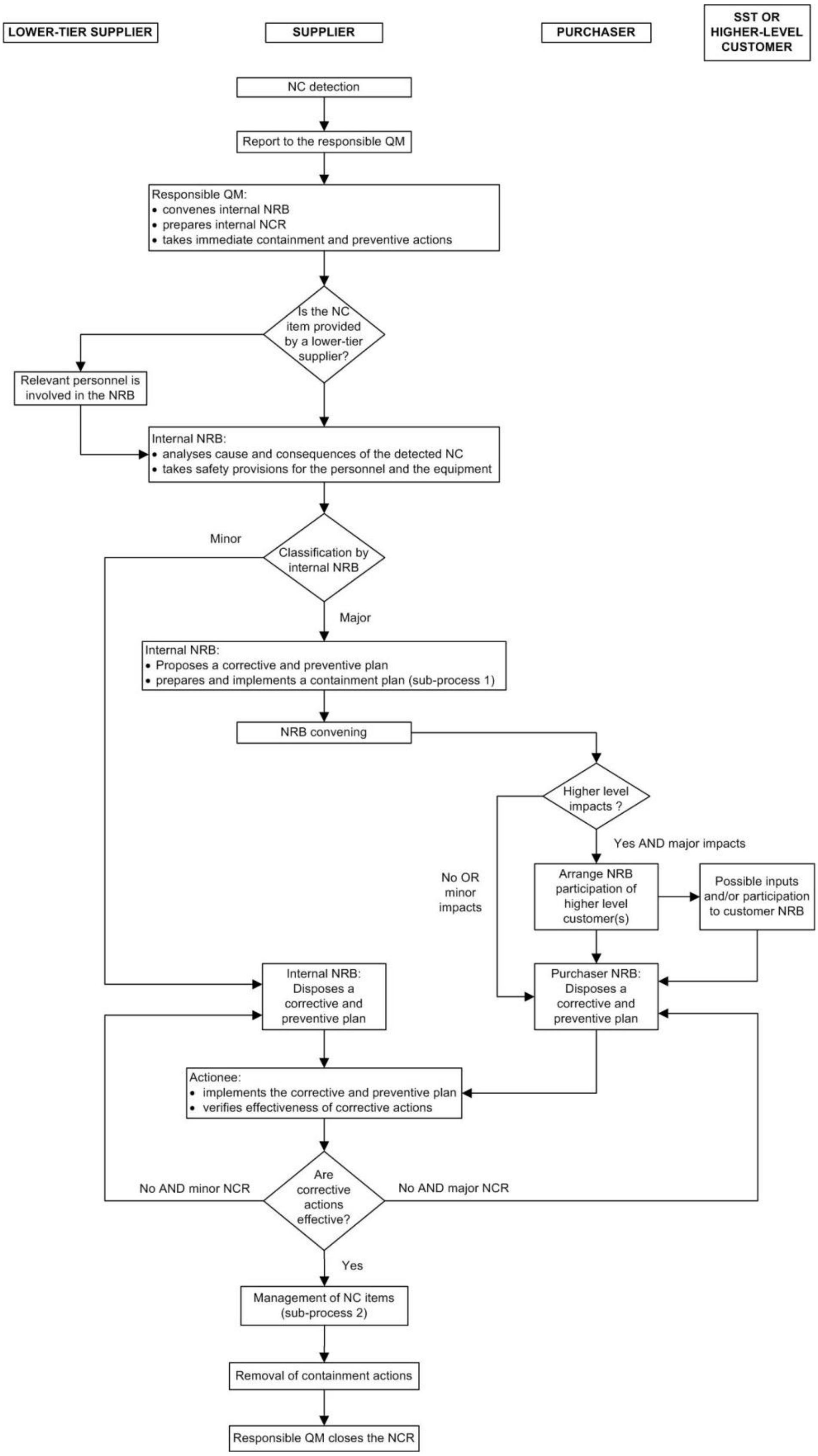
LOWER-TIER SUPPLIER
SUPPLIER
PURCHASER
SST OR HIGHER-LEVEL CUSTOMER
NC detection
Report to the responsible QM
Responsible QM:
• convenes internal NRB
• prepares internal NCR
• takes immediate containment and preventive actions
Is the NC item provided by a lower-tier supplier?
Relevant personnel is involved in the NRB
Internal NRB:
• analyses cause and consequences of the detected NC
• takes safety provisions for the personnel and the equipment
Minor
Classification by internal NRB
Major
Internal NRB:
• Proposes a corrective and preventive plan
• prepares and implements a containment plan (sub-process 1)
NRB convening
Higher level impacts ?
Yes AND major impacts
No OR minor impacts
Arrange NRB participation of higher level customer(s)
Possible inputs and/or participation to customer NRB
Internal NRB: Disposes a corrective and preventive plan
Purchaser NRB: Disposes a corrective and preventive plan
Actionee:
• implements the corrective and preventive plan
• verifies effectiveness of corrective actions
No AND minor NCR
Are corrective actions effective?
No AND major NCR
Yes
Management of NC items (sub-process 2)
Removal of containment actions
Responsible QM closes the NCR

Figure 8-1: Flow-chart of the procedure adopted for the NC management

8.5.1 Management

Any NC detection is reported to the responsible QM, who convenes the internal NRB, takes immediate containment and preventive actions, and prepares a NCR which describes in detail the detected NC. If the NC item is provided by a lower-tier supplier, its responsible personnel (PM, SE, QM) is involved in the NRB. The internal NRB analyses cause and consequences of the detected NC, if necessary, takes safety provisions for the personnel and the equipment, and classifies the detected NC as major or minor:

- Minor NCs are managed directly by the internal NRB, which disposes the corrective actions to eliminate the causes of the NCs, and the preventive actions to avoid the occurrence of the NC on similar items.
- For major NCs, instead, the internal NRB prepares and implements directly a containment plan to isolate the NC items (for HW items only), while proposes a corrective and preventive plan to the purchaser NRB, which takes the final decision. In addition, if the detected NC has a major impact at higher levels, a participation of higher-level customers to the purchaser NRB shall be arranged.

In both cases the Corrective and Preventive Action Plan, the Containment Action plan (if any), and the final fate of the non-conforming items shall be reported in the NCR. The NRB identifies an Action responsible who implements the Corrective and Preventive Action Plan and verifies the effectiveness of the corrective actions: if they are successful the containment actions are removed and the NCR is closed by the responsible QM who opened it, otherwise the actions are revised, implemented and verified again.

8.5.2 Containment Action Plan

The containment action plan is described in Figure 8-2. It shall include (to the extent that is possible in each case) the following steps:

a) After receiving of the NCR, the NRB should locate, identify and quarantine ASAP all nonconforming products and those that could be potentially affected by the same problem, based on the traceability logs and delivery documentation. Locating the NC products means to find out if they are in their own production line, in the warehouse, in transit to the AIV site, in the warehouse of the AIV site or even built in the final product.

b) All quarantined products will be clearly identified with a red label and NCR number and must be checked 100% before using them. The schedule for checking them is determined by the production needs and is independent of the action plans in the NCR. Moreover, if it is decided that in the meantime the production can continue, an inspection of 100 % of produced parts shall be implemented, until the cause of the NC has been identified and corrective actions are verified to be effective.

c) When non-conforming items are procured by a lower-level supplier, the team coordinator shall:
   - Communicate the NC to the lower-level supplier, forward it the NCR and request a list of affected and potentially affected batches. This list shall be delivered by the supplier ASAP.
   - Locate, identify, and quarantine all affected and suspicious products in the warehouse, production line, and finished products at both the team facilities and the AIV site facility
   - Request the lower-level supplier to check all the quarantined products
   - Request the lower-level supplier to check 100 % of all products before delivering them until the cause has been identified and eradicated.

d) When non-conforming items are already delivered to the purchaser, the team coordinator shall:
   - Send to the purchaser a list of affected and suspicious batches that should be quarantined
   - Request to the purchaser to locate, identify, and quarantine all affected and suspicious items
   - Request to the purchaser to check all the quarantined items

In all cases a report on the checked NC items and on the inspected newly produced items (if any) shall be provided.

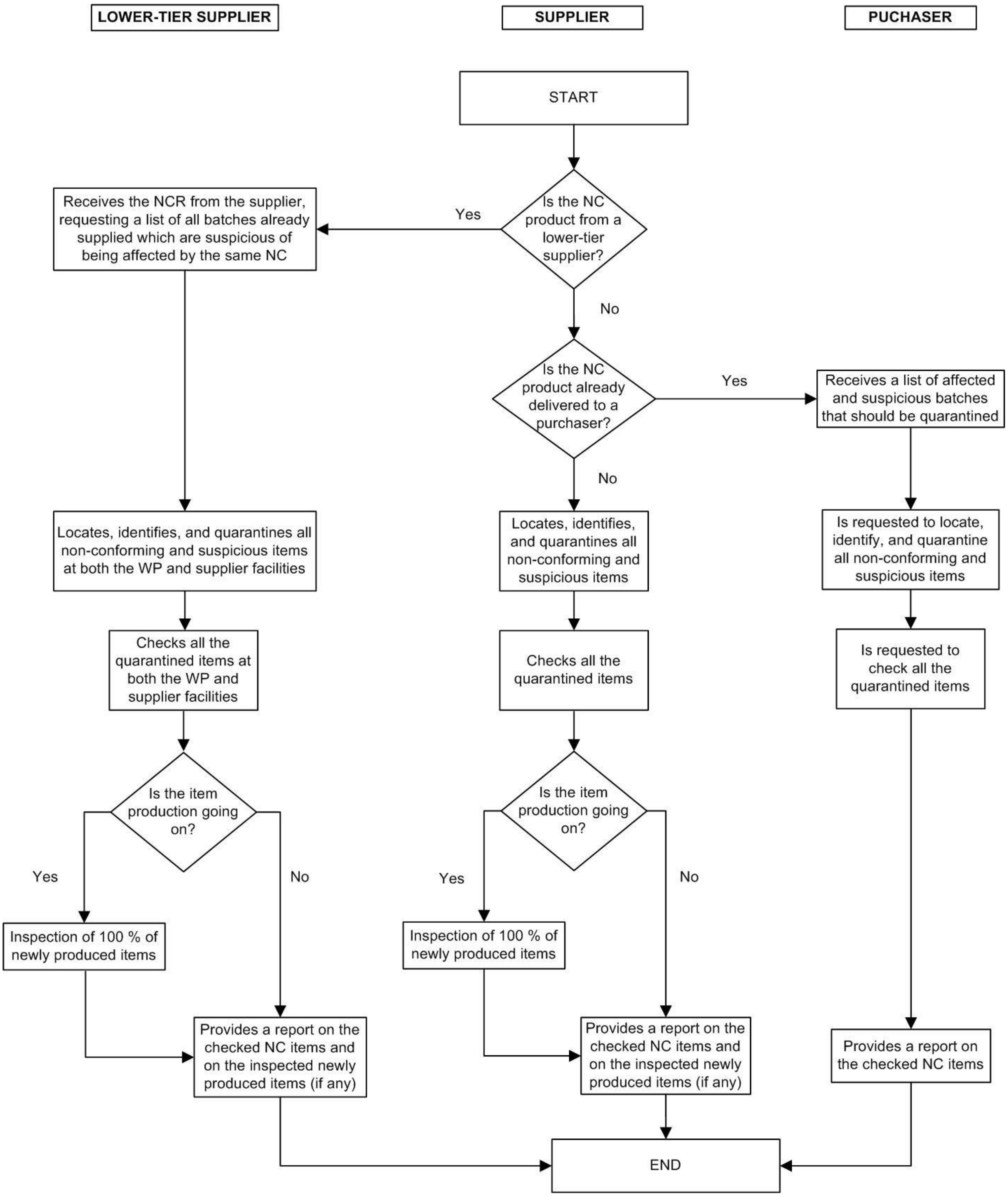
LOWER-TIER SUPPLIER
SUPPLIER
PUCHASER
START
Is the NC product from a lower-tier supplier?
Yes
No
Receives the NCR from the supplier, requesting a list of all batches already supplied which are suspicious of being affected by the same NC
Is the NC product already delivered to a purchaser?
Yes
No
Receives a list of affected and suspicious batches that should be quarantined
Locates, identifies, and quarantines all non-conforming and suspicious items at both the WP and supplier facilities
Locates, identifies, and quarantines all non-conforming and suspicious items
Is requested to locate, identify, and quarantine all non-conforming and suspicious items
Checks all the quarantined items at both the WP and supplier facilities
Checks all the quarantined items
Is requested to check all the quarantined items
Is the item production going on?
Yes
No
Is the item production going on?
Yes
No
Inspection of 100 % of newly produced items
Inspection of 100 % of newly produced items
Provides a report on the checked NC items and on the inspected newly produced items (if any)
Provides a report on the checked NC items and on the inspected newly produced items (if any)
Provides a report on the checked NC items
END

Figure 8-2: Flow-chart for the containment plan of the NC items (sub-process 1 of Fig. 8-1)

The team coordinator might also provide additional information (photos, defect samples, special test instructions) for helping the purchaser to identify the affected products.

8.5.3 Corrective Action Plan

The corrective action plan (applicable also to lower-level suppliers) includes the following steps:

a) The NRB will investigate the causes of the nonconformity and design a solution to eradicate the problem.
b) If it is decided that in the meantime the production can continue, an inspection of 100 % of produced parts should be implemented.
c) The NRB implements the solution and checks its efficacy (for example, by inspecting at least 20 % of produced parts): if the corrective actions are effective, the revision of the new parts is removed and the NCR is closed, otherwise the causes of the nonconformity are investigated again and a new solution to eradicate the problem is designed.

8.5.4 Management of NC items

In Figure 8-3 the flow chart to manage the NC items is reported.

If the NC item is internally produced, if possible, it is reworked or repaired and delivered to the integration site. If, on the other hand, no rework or fixing is possible, but the NC item can be used as it is, a RFW is sent to the purchaser: if the purchaser accepts the RFW, the configuration data sheet of the affected item is updated, the item is labelled with the corresponding waiver reference and it is delivered for further integration; if, on the other hand, the purchaser rejects the waiver, the NC item is scrapped. A NC item which cannot be used as it is, shall be scrapped as well. It is expected that this last possibility is applicable only to HW items, since in the SW case any NC item can be repaired or reworked.

If the NC item is provided by a lower-level supplier, the relevant personnel (PM, SE, QM) is involved in the NRB to agree with the upper-level supplier the fate of the affected items.

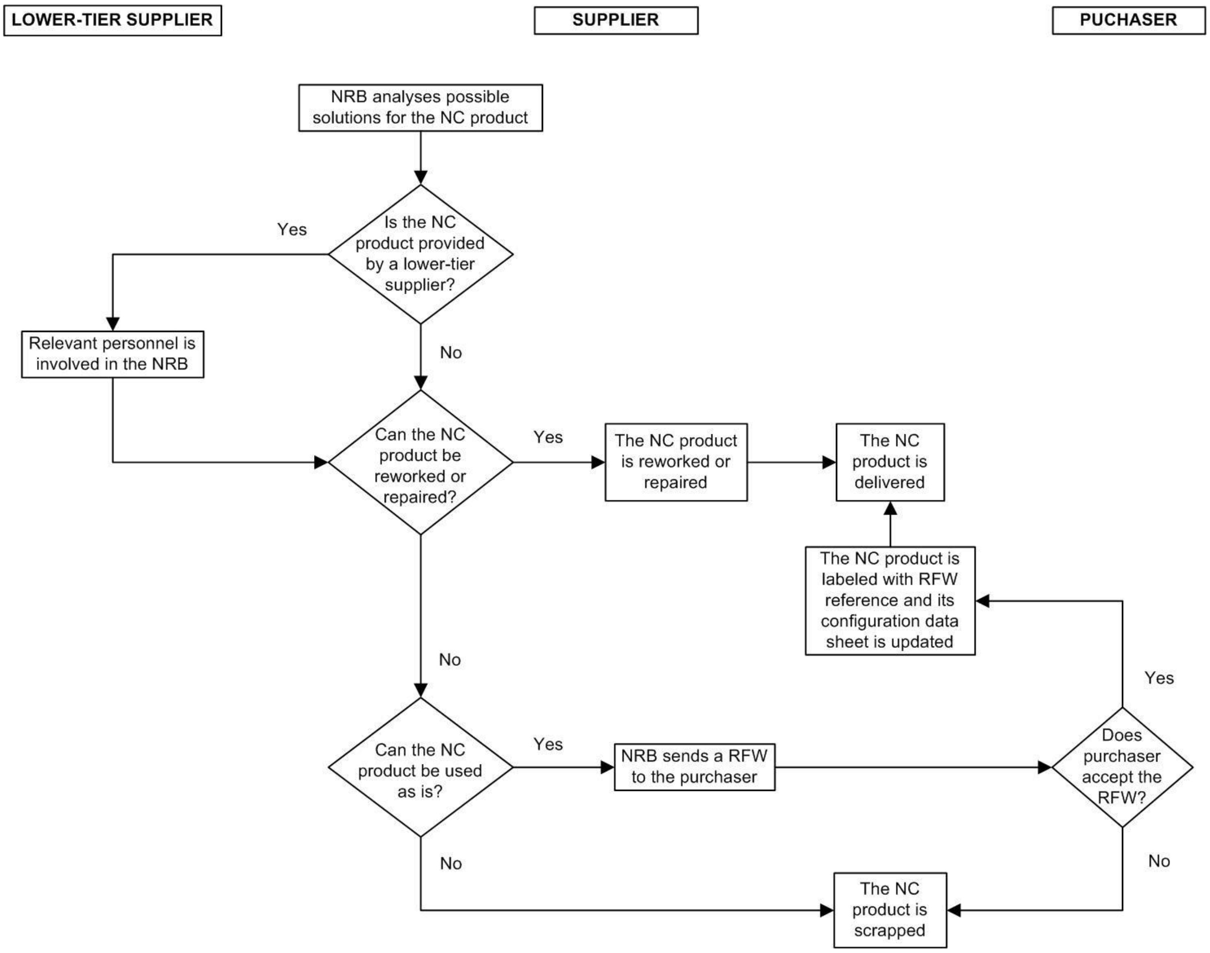
LOWER-TIER SUPPLIER
SUPPLIER
PUCHASER
NRB analyses possible solutions for the NC product
Is the NC product provided by a lower-tier supplier?
Yes
Relevant personnel is involved in the NRB
No
Can the NC product be reworked or repaired?
Yes
The NC product is reworked or repaired
The NC product is delivered
The NC product is labeled with RFW reference and its configuration data sheet is updated
No
Yes
Can the NC product be used as is?
Yes
NRB sends a RFW to the purchaser
Does purchaser accept the RFW?
No
No
The NC product is scrapped

Figure 8-3: Flow-chart for the management of NC items (sub-process 2 of Fig. 8-1)

8.5.5 Non-Conformance close-out

The NCR can be considered closed when all agreed dispositions/actions have been successfully implemented and verified. All analyses requested by the NRB will be completed before the closure. The analysis reports will be submitted to NRB for review in advance with respect to the NRB date.
In order to close the NCR, it shall be signed by all the members of the NRB and of the SST management (QM responsible, WP manager, SE, PM). In addition, in the case of external suppliers, the NCR shall be signed also by the Lead Partner responsible for the contract.

9 RAMS

During the SST construction, a reliability analysis will be implemented since the design phase, in order to guarantee fulfilment of the availability requirement of the instrument during its lifetime. Each subsystem will carry out this analysis coordinated by the SST RAM manager. A RAMS plan will be prepared to carry out the activities related to this topic. RAMS activities will be implemented since the starting point of the project and will be part of the progress reports and reviews.

9.1 Dependability evaluation

The following analyses are used for determining reliability, maintainability and availability requirements and tasks:

- Failure Modes, Effects, and Criticality Analysis (FMEA/FMECA) with identification of Single Point Failures (SPFs) and failure propagation;
- Hardware Software Interaction Analysis;
- Parts Stress Analysis (Parts Application Review);
- Worst-Case Analysis;
- Reliability Assessment;
- Fault tree analysis;
- Common cause and Common mode analysis.

All activities will be carried out in parallel to the design process in close co-operation with design engineers.

9.2 Reliability evaluation

To identify all failure modes of the system and rank them in accordance with the severity of the effects of their occurrence a comprehensive Failure Modes, Effects and Criticality Analysis (FMECA) shall be performed on the functional and physical design (functional FMECA and design FMECA) of the entire instrument. In all cases the FMEA/FMECA will identify how each failure mode is detected.

The FMECA activity will be carried out in a systematic way to ensure that all items and their interfaces are adequately addressed. Lower level FMECA will be used as input in a build-up process to generate the higher level FMECA.

FMECA shall be carried out for all operational modes of the instrument.

The following Failure Effect Severity Categories related to dependability will be used in the FMECA:

- CATASTROPHIC: Propagation of failure to other subsystems / assemblies / equipment
- CRITICAL: Complete Loss of functionality.
- MAJOR: Degradation of functionality.
- MINOR: Any other effect.

The following attributes shall be added to the criticality category as appropriate:

- the suffix “S” shall be used to indicate safety impacts.
- the suffix “R” shall be used to indicate redundancy
- the suffix “SP” to indicate Single Point Failure

A Single Point Failure is an item for which no redundancy or back up is implemented in the design. Such item is identified with a suffix “SP” in the FMEA/FMECA. Single Point Failures with severities 1, 2 and 3 and failures with risk of propagation (at upper level or to internal redundancy) will be considered as critical items and will be processed as such in the CIL.

As output of FMECA analysis, Single Point Failures will be potentially identified. A list will be implemented with the aim to solve or mitigate their effects. If it is not possible to avoid them, a final list with probability and occurrence will be delivered.

A FMECA report will be supplied and updated in accordance with the contract. The FMECA will include the following information:

- a narrative description of product functions to provide an understanding of the analysis;
- block diagrams and schematics to assist in describing the product (functional block diagrams, reliability diagrams);
- definition of the status of the design of the product under analysis;
- basic rules and assumptions adopted for the analysis;
- failure detection and isolation criteria;
- results and recommendations based upon the detailed analysis presented by the FMECA worksheets;
- a list of all the critical items identified;
- a list of all the failure effects leading to consequence classified as catastrophic, critical, or major;
- status of recommendation;
- FMECA worksheets.

The FMECA worksheets will include for each analysed item:

- Identification;
- short description of the function;
- assumed failure mode;
- possible failure causes (when available);
- effects on mission;
- observable symptoms;
- existing preventive or compensation measures;
- criticality level and suffix according to ECSS recommendations and remarks.

The results of the FMECA will be used as input to the design reviews and for implementing corrective actions. An update FMECA will be submitted at each instruments design review.

Principles, requirements and procedures to apply FMEA/FMECA are described in ECSS-Q-ST-30-02C.

If needed the FMEA/FMECA will be completed by the following analyses:

- Fault Tree Analysis (FTA), a top-down analysis allowing the identification of failure combinations that can lead to events with catastrophic consequences.
- Common-cause and Common-mode analysis on reliability and safety critical items (ECSS-Q-ST-30C), to identify the root cause of failures that have a potential to negate failure tolerance levels.

9.3 Maintainability

By analysis of the requirements on operation lifetime, hardware configuration and Mean Time Between Failures (MTBF) of the subcomponents, a maintainability plan will be carried out. In particular, as product of this analysis a spare list and a maintenance (preventive and corrective) manual will be delivered. Preventive maintenance will assure that reliability requirements will be fulfilled. Corrective maintenance assures that instrument downtime will be inside specifications.

9.4 Safety Assurance

Aims of the safety assurance program are:

- to identify hazards for personnel;
- to eliminate hazards or to mitigate them to an acceptable level;
- to assure compliance with safety requirements and rules

The safety assurance program [RD02] will cover all the phases of the project (design, manufacturing, assembly, testing, transportation and operations).

As output of the safety assurance program, a hazard analysis document will be delivered, containing the hazard item list with the associate risk level and actions to be implemented to mitigate them.

10 Appendix: template for Non-Conformance Reports

The following template will be used to track NCRs:

Table 10-1: Template for the Non-Conformance Reports

NCR No.: SST-NCR-XXXX-YYY (see RD1) NCR type: Major/Minor	Revision: Date:
NCR Title:	
NC item (name/serial number):	
Procedure (with code) or activity in execution when NC occurs:	
Description of Non-conformance: Description of the problem and of the occurrence conditions (HW/SW configurations, environmental conditions, test set-up, …) Reported by: Requirements violated (if any):	
Cause of NC:	
Remedial Action: Description of possible solutions adopted to proceed with the on-going activity Action by: action responsible	To be completed by: due date
Action to Prevent Recurrence: Description of possible solutions adopted to avoid repetition of the same problem on similar items Action by: action responsible	To be completed by: due date
Corrective Action: Description of the solution adopted to remove the problem causes Action by: action responsible Verified by: who verifies the action effectiveness	To be completed by: due date name signature

NCR close-out			
Name	Position	Signature	Date
	Responsible WP Supplier		
	Responsible QA Supplier		
	PM Supplier		

	Responsible SST WP		
	Responsible SST sub-WP		
	Responsible QM for SST WP		
	SST Programme QM		

END OF DOCUMENT