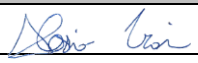
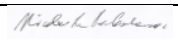
SST Programme
Safety Management Plan

SST-PRO-PLA-006

Version 2a

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

Current Release				
Ver.	Created	Comment	Distribution	Editor(s)
2a	20/07/2023	Updating and Re-issuing of the document	SST Consortium	Fatima De Frondat (OP-INSU)

Version History				
Ver.	Created	Comment	Distribution	Editor(s)
1a	14/11/2022	First issue of the document	SST Consortium	N. La Palombara (INAF)
2a	20/07/2023	Updating and Re-issuing of document	SST Consortium	Fatima De Frondat (OP-INSU)

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Propose and objective

This document defines the safety management policy to be adopted during the consolidation and construction phase of the CTA SST Programme (SST-PRO). It describes how to fulfil the specified safety requirements aiming to protect the personnel, the product and the environment from hazards associated with the SST-PRO activities.

The objective of this document is to ensure that all safety risks associated with the delivery, erection, operation and maintenance of SST equipment are adequately identified, assessed, minimized, controlled and finally accepted through the implementation of the present document.

1.2 Scope

This document covers the following:

- CTA SST System Safety objectives and approach;
- Safety programme description and organization (tasks to be implemented, roles and responsibilities for the execution of those tasks);
- the schedule of system safety programme tasks related to project milestones and phases
- the Safety engineering procedure followed by the SST partners and contractors to accomplish the tasks and verify satisfactory completion
- Safety verification;
- Operational safety;

Each SST partner and / or contractor shall establish and maintain a safety programme consistent with this SST Safety Management Plan, in order to assure conformance with project safety policy and requirements.

This SST Safety Management Plan is a living document that must be revised as needed. It's applicable for the next Programme phases as described in [AD3], i.e. from the Consolidation Phase up to the AIV Phase and telescopes hand-over to CTAO. The present document is applicable to all deliverables and activities by In-Kind contributors and doesn't include:

a) The occupational safety and health aspects (OSH aspects). These OSH aspects are under the responsibility of the site officer and will be described in another document.
b) The Construction Site safety. These aspects are under the responsibility of CTAO and will be defined by the Constructions Site Manager and the Construction Site Safety Engineer.

This document concerns the product safety relevant to the items that must be delivered to CTA. In particular, it applies to:

- the item manufacturing, assembly, integration and laboratory test
- the item packing, shipping and unpacking at the system integration site
- the item handling and maintenance

This document applies to the system integration, commissioning and operation.

1.3 Applicable Documents

[AD1] CTA-SPE-TEL-000000-0003_1a -Telescope safety design specifications

[AD2] CTA-PLA-MGT-000000-0003_1c I.1.2 - CTA Project Management Plan

[AD3] SST-PRO-PLA-001 - SST Programme Project Management Plan

[AD4] CTA-PLA-SEI-00000-0001 I.1a - CTA System Safety Program Plan

[AD5] CTA-TRE-SEI-00000-0001 I.1a - CTA Project Phases Specific Safety Activities

[AD6] SST-PRO-PLA-005 1a - SST Programme PA & QA Plan

1.4 Reference Documents

[RD01] SST-PRO-SPE-001 - Telescope Technical Requirements Specification

[RD02] SST-STR-SPE-002 - Structure Requirements Specification

[RD03] SST-OPT-SPE-002 - Optics Requirements Specification

[RD04] SST-MEC-SPE-002 - Mechanics Requirements Specification

[RD05] SST-CAM-SPE-002 - Camera Requirements Specification

[RD06] SST-PRO-DSR-001 - Telescope Design Report

[RD07] SST-OPT-DSR-001 - Optics Design Report

[RD08] SST-MEC-DSR-001 - Mechanics Design Report

[RD09] SST-CAM-DSR-001 - Camera Design Report

[RD10] SST-STR-PLA-009 - SST-STR Engineering Development and Verification Plan

[RD11] SST-CAM-PLA-009 - SST-CAM Engineering Development and Verification Plan

[RD12] standard DIN EN ISO 12100 and ISO/TR 14121-2

1.5 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 (15 February 2017)

1.6 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
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
EEA	European Economic Area
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
HTS	Hazard Tracking System
IACTs	Imaging Atmospheric Cherenkov Telescopes
IKC	In Kind Contribution
INAF	Istituto Nazionale di Astrofisica
KO	Kick-Off
MAIV	Manufacturing, Assembly, Integration and Verification
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
PRR	Production Readiness Review
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
SSO	System Safety Officer
SSPP	System Safety Program Plan
SST	Small Size Telescope
SST-CAM	SST Camera
SST-PRO	SST Programme
SST-STR	SST Structure

TRR	Test Readiness Review
VCD	Verification Control Document
WBS	Work Breakdown Structure
WP	Work Package
WPD	Work Package Description

2 SST Safety Management objectives and approach

The objective of safety management process is to ensure that all safety risks associated with the design, development, production and operations of CTA SST telescopes are adequately identified, assessed, minimized, controlled and finally accepted through the implementation of a safety management programme.

2.1 Safety approach

In accordance with the directive 2006/42/EC on machinery and [AD01], the CTA SST System safety policy is to:

- ensure that SST telescopes do not cause a hazard, in descending order of priority, to:
  - human life,
  - the environment,
  - the telescope items
- determine and evaluate the safety risks associated with the project activities,
- minimize safety risks in a technically effective and cost-effective manner,
- ensure adequate verification of safety control measures.

CTAO, as European Research Infrastructure, has adopted the European product safety legislation as applicable legislation for the products produced and used at the CTA North and South sites. This means that all products and parts of products delivered to CTAO must - independently of the final place of use - fulfil the European product safety requirements applicable for products produced for the extended Single Market in the European Economic Area (EEA)[1].

On this ground the CTA Contributors must apply European product safety legislations, which are transformed by the EU member states into national laws.

The consequences for the SST Programme are:

- All parts or the final products that will be delivered to the CTA-South site must comply with the EU product safety legislation plus ESO specific safety requirements[2];
- Each In-Kind Contributor, other SST partners and / or supplier is responsible for the compliance of their produced products to the applicable European product safety legislation, and the fulfilment of the CTAO safety requirements during all project phases;
- The EU product safety legislation including the safety assessment processes must be applied by all Partners during all project phases;
- The EU Safety Conformity Assessment Procedure must be followed from the beginning of the Preliminary Design Phase throughout all project phases.

[1] See http://ec.europa.eu/growth/single-market/ce-marking_en

[2] It is assumed that ESO requirements are compliant with Chilean legislation

The implementation of safety requirements shall not be compromised by other requirements.

2.2 Safety programme

The CTA SST System safety policy is implemented by applying a safety programme, which ensures that:

- Safety precautions are considered to deliver a safe design complying with the EHSRs of all applicable EU Directives and the appropriate harmonized EN standards as described in [AD1]
- safety-related risks with respect to the design, development and operations of the SST telescopes are identified, assessed and controlled based on qualitative and quantitative analysis as appropriate;
- safety controls are adequately implemented,
- safety requirements are met,
- application of a hazard reduction precedence and of control measures of the residual risks.

3 SST-Programme Safety Organization

This section describes the organizational context, both technical and managerial, within which the prescribed SST System safety activities shall be implemented, and the tasks and responsibilities of the responsible actors. It is based on the managerial structure of the SST-PRO described in the SST Programme Project Management Plan [AD3].

3.1 Organization Chart

The organization chart for the safety management of the SST-PRO is reported in Figure 3-1.

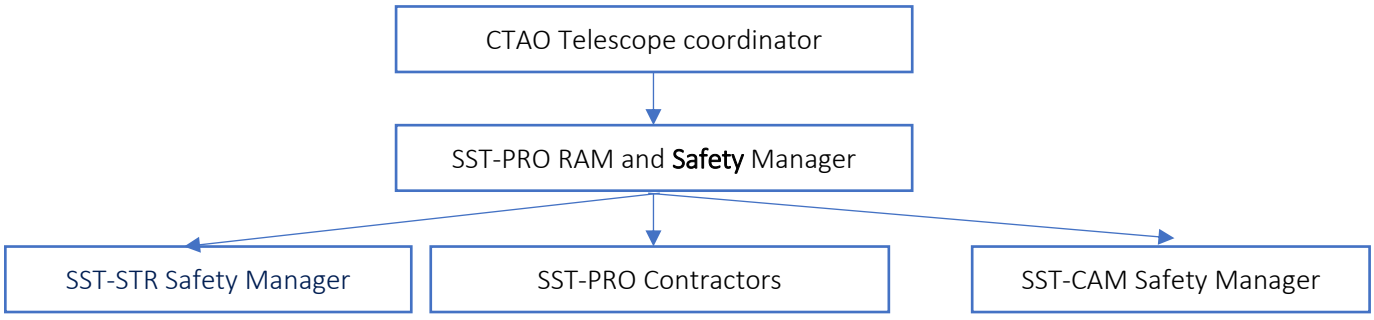


Figure 3-1: SST System Safety organization

3.2 SST-PRO Safety Managers team

As mentioned in the project WBS, Safety management is part of the RAMS Manger perimeter

Projects (structure and camera) shall appoint an internal Safety Manager.

The SST Industrial Contractors, for the execution of their product safety duties and responsibilities during the design and production processes, shall nominate a Product Safety Manager.

SST-Safety Managers acts in a best-effort fashion and bears no legal responsibility for ensuring complete safety coverage, or for institutes properly implementing the recommended procedures (the burden of which rests with local PIs and safety officers)

3.3 Safety Tasks and Responsibility

3.3.1 Safety Programme Manager

3.3.1.1 General tasks

The Safety management activities are under the responsibility of the SST-PRO RAMS Manager. She is responsible for:

- the definition of the safety management plan,
- the coordination of the Safety Managers team
- the monitoring and control of the overall system safety activities. this can be done if needed in interface with others relevant expertise in the project (ie: System Engineer, PA Manager etc.)
- report on safety Matter to CTAO safety contact and SST-PRO PM

3.3.1.2 Responsibilities

The SST-PRO Safety Manager acts during the entire construction phase and shall have organizational authority and independency to:

1) manage - in close cooperation with the project safety managers and relevant expertise - all safety assurance aspects (including software) during the construction Phase
2) coordinate the safety related interfaces:
   a) with the relevant SST Institutes and Contractors
   b) with ESO
   c) with CTAO
3) monitor and control the correct execution of the present safety management plan at SST projects institutes and contractors
   4) Convening and chairing system safety related meetings
   a) Defining applicable system safety requirements, and tools in line with CTAO safety requirements

3.3.1.3 Access

The SST-PRO Safety Manager:

1) has the right of access to all safety-related data relevant to SST-Projects safety system,

2) has unimpeded access to any management level without organizational constraint on any aspect of SST Projects safety.

3.3.1.4 Authority

The SST-PRO Safety Manager has the authority to:

1) manage, review and approve final safety documents that should be delivered to CTA and or ESO.
2) order the cessation of any project activity on any SST-related site, that does not conform to approved safety requirements or procedures,
3) order the interruption of hazardous operations on any SST related site when the operation or the product does not conform to the agreed measures defined in the corresponding hazard report.
4) accept the statement of the programme safety compliance

3.3.1.5 Representation on Boards

The SST-PRO Safety Manager shall be present on boards where safety and / or health aspects are involved. This includes the non-conformance review boards (NRBs), test review boards (TRBs), qualification and acceptance reviews, where safety requirements and safety-critical functions are involved. During the board's meetings, if needed, the SST-PRO Safety Manager can be assisted by the relevant SST project safety manager and / or contactor Safety Manager.

The execution of the SST safety management programme is the responsibility of the project safety managers as defined in the figure 3-1 above.

3.3.2 Safety Management in the SST Structure (SST-STR)

The SST-STR Safety Manager shall have on his/her sites the necessary authority to implement the Safety Management Plan at his/her sites, monitor and control its execution.

The SST-STR Safety Manager reports to the SST-PRO Safety Manager about product safety-related matters. Safety progress reporting is part of the standard progress reporting activity.

For critical and / or Major hazard safety related a "Red flag report" shall be communicated to the SST-PRO Safety Manager immediately and at the latest within three days following occurrence of hazard problem. A meeting is then organised with the presence of relevant expertise and authority. Hazard description and actions are registered by the SST-STR Safety Manager in the SST-STR Hazard Reporting and Tracking System as defined in section 7.2, or any other tool agreed. This does not apply to occupational health and safety related incidences.

3.3.2.1 General Tasks and Responsibilities

The SST-STR Safety Manager shall have organizational authority and independency to implement this Safety Management Plan.

In particular, the SST-STR Safety Manager is responsible for:

- Monitoring and control the correct execution of the SST System Safety Management Plan at all the SST-STR Project-related Institutes and Contractors

3.3.2.2 Access

1) has the right of access to all safety-related data relevant to SST-STR Project safety,
2) has unimpeded access to any management level without organizational constraint on any aspect of the SST-STR safety.

3.3.2.3 Authority

The SST-STR System Safety Manager shall have the authority to:

5) reject any project document, or to stop any project activity on SST-STR site, that does not conform to approved safety requirements or procedures,
6) interrupt hazardous operations on any SST-STR-related site when it becomes clear by the System Safety Manager that the operation or the product does not conform to the agreed measures defined in the corresponding hazard report Safety Approval Authority

The SST-STR System Safety Manager shall have the authority to:

1) review and approve all documents dealing with SST-STR safety matters
2) review and approve any hazardous operation before it is executed
3) generate the safety related project progress reports
4) review and dispose any safety data submittals
5) approve the close-out of hazards
6) decide on deviations and waivers, jointly with the SST-PRO Safety Manager
7) accept the statement of the SST-STR safety compliance.

3.3.3 Safety Management in the SST Camera (SST-CAM)

The SST-CAM Safety Manager is responsible for the flow down of safety planning from the Programme level to the camera team institutes.

A list of safety officers (1 per institute) will be maintained by the SST-CAM Safety Manager.

The SST-CAM Project will implement detailed procedures for common operations that follow the standards in Section 5.

Each team (institute) will consider these procedures in preparing their SOWs for delivering their parts of the WBS (i.e. the appropriate ones are applicable to those SOWs).

Each team (institute) will review the applicable procedures with their local safety officer, and adapt for local use if needed.

All activities at individual institutes should follow local (legal) rules.

Following an incident, the local safety office follows local rules. They inform the local PI and the SST-CAM Safety Manager, who informs the SST-PRO safety manager, the camera PM and Board.

3.3.4 Safety Management Interfaces

The Safety Manager of each Project (SST-STR and SST-CAM) interfaces directly with all members of his/her Project and the related project management disciplines, ensuring that the contractual provision

and schedule planning for the definition and phasing of safety activities are met. If needed and accepted, the safety Managers of each project can also interface with the contractors Safety Managers.

The SST-PRO Safety Manager interfaces directly with the safety manager of each SST Institute or Contractor regarding all safety-related matters and keeps the SST-PRO PM appropriately informed about Safety matters.

3.3.5 Safety Audits

In order to guarantee the product, safety audits may be performed where required and appropriate by the SST-PRO Safety Manager (or by someone designated by him) at the contributor's site. Safety audits are reviews to verify compliance to the described SST System Safety Management Approach (2.2) and specified safety policy and requirements.

Safety Audits will be planned when necessary to review the execution of the safety programs and to overcome safety problems, constant poor quality of safety activities, or other problems.

3.4 Constraints and Requirements placed on Project / System Safety

This section lists the "external" safety-related constraints and requirements placed on the Projects and the entire system. All Safety requirements and standards listed in [AD1] are applicable throughout the entire project

3.4.1 Legal Safety Requirements

3.4.1.1 Occupational Health and Safety (OHS)

The national OHS legislation applicable at the location of the Project activity is applied for the activity.

The local execution of the relevant OHS legislation at the places involved in SST activities is not subject of this program.

3.4.1.2 Product / Equipment / System Safety

The EU Product Safety Legislation formulated in the various EU Directives, e.g. the EU Directive 2001/95/EC on general product safety, is applicable throughout the entire project.

3.4.1.3 Hosting Agreement Safety Requirements

CTA-South: The contractual safety requirements related to CTA-South are defined in the ESO - CTAO Hosting Agreement.

3.5 Safety hazard assessment and control

The safety hazard identification, reduction and control are part of the RAMS management process.

Safety hazard identification, reduction and control is a continuous and iterative process throughout the project life cycle, encompassing:

1. allocation of safety requirements;
2. hazard and safety hazard identification;
3. evaluation (including categorisation) of consequence severity;
4. hazard and safety risk reduction and control;
5. close out and acceptance of residual hazard.

For the identification of hazards and associated safety risks, consideration shall be given to past experience, studies, tests, reviews, industrial process as well as the operational use.

3.6 Project phases and safety review cycle

Safety analysis shall support preliminary design, detailed design, production, qualification, integration, and acceptance phases, up to the delivery of the SST telescopes to CTAO.

3.7 Operational Safety

When working at the CTA Observatory in Chilli the local and ESO Safety regulations are applicable in addition to the CTA safety processes.

3.8 Safety of ESO Loaned and Furnished Property (if any)

The equipment loaned from ESO or provided by ESO for use in the Project as part of the installation activities shall conform to the safety requirements and principles of the ESO Technical Specification and of this safety management plan. ESO is responsible for performing the necessary safety compliance assessments for its equipment, and for demonstrating the safety compliance to the CTAO during the hand over process.

3.9 COTS and Third Party Produced Items

Commercial-off-the-shelf (COTS) items and items produced by third parties shall comply with the EU Product Safety Legislation.

3.10 Safety compliance demonstration

Each SST partner and / or supplier shall provide a statement of safety compliance to demonstrate that the system elements conform to stated safety requirements.

The project shall provide to the CTAO safety approval authority all safety-related information for their acceptance of the statement of safety compliance.

3.11 Safety training

3.11.1 General

Safety training shall be part of the overall training.

All safety-related training of any personnel working – permanently or occasionally – with system elements that can have hazardous properties shall have three major aspects:

1) General awareness briefings on safety measures to be taken at a given location or working environment
2) Basic technical training in the required safety techniques and skills, which is a prerequisite to fulfil the job function under consideration (for example: inspection, test, maintenance or integration)
3) Product specific training that focuses on the hazards related to the specific system element

3.11.2 Product specific training

Each project shall identify the need for product specific safety training and implement the corresponding safety training programme for all relevant parties.

3.11.3 Basic technical training

Each project shall provide basic technical training to all project engineering and safety personnel working with hazardous products.

3.11.4 Training records

Each project shall maintain records of personnel having received safety training.

3.12 Accident-incident reporting and investigation

Each project shall report to the SST-PROM all accidents and incidents occurred during project activities under the control of the project itself or its lower-tier SST partners that affect the system element.

Each project shall support – at request – project-related accident and incident investigations that occur outside of the project's control or facility.

The accident or incident investigation report shall be formally closed by the project upon approval by the SST-PRO.

If the conclusion of the assessment is that the accident-incident has had an effect on the project, i.e. the safety of the product or its operation, the organisations safety representative shall be informed.

In the previous case, the accident-incident report shall become part of the project's safety data and shall be documented in the safety data package.

3.13 Safety documentation

3.13.1 General

Each SST project and contractor/supplier shall maintain, as part of the project documentation, all safety-related data to support reviews and safety compliance demonstration.

The following Safety Documentation Package shall be delivered by each SST-Project and supplier in line with the requirements and methodology mentioned in [AD1]

- Hazard Analysis
- Hazard Material List
- Safety Compliance Assessment Report
- Fault tree analysis (FTA)
- Safety progress report
- "Safety Red flag report if any"
- deviations and waivers reports if any
- Safety assessment report following the cotenant expected by Safety Approval Authority for each review.
- All other document requested by CTAO in the next project phases

The documentation above are part of a continuous and iterative process it shall be updated as needed throughout the SST-PRO life cycle. When a template is existing, it shall be used and completed. Periodic safety progress shall be delivered to the SST-PRO Safety manager with the last version up to date of the documentation above.

3.13.2 Safety deviations and waivers

3.13.2.1 Request for deviation or waiver

Safety requirements that cannot be met shall be identified by contractors / suppliers.

A relevant request for deviation (RFD) or waiver (RFW) shall be generated and tracked.

3.13.2.2 Assessment of deviation or waiver

All RFDs/RFWs shall be assessed in order to identify those, which impact safety.

The accumulated deviations and waivers that affect safety shall be assessed to ensure that the effects of individual deviations and waivers do not invalidate the rationale used for the acceptance of other deviations and waivers.

3.13.2.3 Acceptance by the safety approval authority

Safety deviations and waivers shall be subject to acceptance of the safety approval authority.

3.13.2.4 Review and disposition

Deviations and waivers that affect project safety requirements or safety-critical functions, which the SST partner and / or contractors consider acceptable, shall be subject of review and disposition by the SST-PRO and the safety approval authority.

4 Safety and Project Engineering Activities

This section outlines the concurrent safety and project engineering activities in continuous support of the Project design and development and of manufacturing, assembly, integration and verification (MAIV) processes.

4.1 Design Consolidation Phase

Safety analysis and risk reduction activities shall support the detailed design. These safety activities shall also support operational safety optimization, safety requirements implementation evaluation, risk reduction verification, hazard and risk acceptance.

Analysis of operations shall also support the identification of emergency and contingency response planning and training requirements, and the development of corresponding procedures.

The projects and Contractors, coordinated by the SST-PRO safety Manager, shall:

1) prepare a safety assessment report summarizing the status of the safety activities and highlighting safety matters needing special attention during the following project phase
2) prepare the safety related input for:
   (d) Design Configuration Baseline established following the CDR
   (e) CDR documentation
   (f) safety activity planning for the following project phases
3) participate in CCB and other project meetings as required.

4.2 Production and AIT/V Phase

Safety analysis and risk reduction activities shall support the manufacturing, assembly, integration, and tests activities.

As needed each SST project and contractor's / supplier's safety manager-coordinated by the SST-PRO Safety Manager- shall:

1) prepare a safety assessment report summarizing the status of the safety activities and highlighting safety matters needing special attention during the following project phase
2) prepare the safety-related input for
   (a) user and maintenance manuals,
   (b) transport, shipping, installation and commissioning documentation
   (c) Product Configuration Baseline established following the internal product acceptance
   (d) Preliminary acceptance documentation

(e) Safety activity planning for the following project phases

3) participate in CCB and other project meetings as required
4) participate to the organisation of safety training for users and maintenance staff
5) participate in MAIV safety inspections and tests
6) participate in preliminary acceptance related activities
7) prepare the CE Compliance Assessment document

4.3 Transport and Shipping

In addition to the safety compliance assessment activities, the System Safety Manager as well as the Institutes and Contractors shall have the right to:

1) monitor the safety-related transport and shipping activities, whereby the transport safety responsibility remains with the contributors.
2) participate in project meetings as required
3) participate in CTA South site incoming inspections

4.4 On-site AIT/AIV Phase

Safety analysis shall evaluate design and operational changes for impact to safety, assuring that safety margins are maintained and that operations are conducted within accepted risk.

The analysis shall also support the evaluation of operational anomalies for impact to safety and the continued evaluation of risk trends.

In addition to the safety compliance assessment activities at System and Subsystem level, the System Safety Manager, in cooperation with the site safety officer, shall:

1) Participate, to the training organization of the Institutes and Contractor staff in observatory safety regulations
2) perform safety-related inspections and tests
3) monitor the safety-related reintegration and installation activities
4) participate in project meetings as required

4.5 Final Acceptance

Final acceptance of each deliverable telescope is performed at the CTA South site at the end of the AIT/AIV phase and is documented by an acceptance certificate.

By signing the acceptance certificate, CTAO confirms that the delivered telescope complies with the contractually specified requirements. Each SST project and contractor / supplier is responsible for the conformity of the product he deliver.

The CE Conformity Declaration is an essential safety verification document for the acceptance act.

5 Safety engineering procedure

5.1 Overview

Safety engineering consists of safety analysis, management of hazard and risk reduction processes, hazard and risk potential assessment, design assurance, and hazard and risk control activities.

5.2 Safety requirements identification and traceability

Safety requirements shall be identified and traced from the system level into the design and then allocated to the lower levels.

When specified by the project, the identified safety requirements shall be justified in the design and presented in an appropriate document.

5.3 Safety design objectives

5.3.1 Design selection

Appropriate design features shall be selected to ensure inherent safety. Such features are fail-safe design solutions, damage control, containment and isolation of potential hazards.

5.3.2 Hazard reduction precedence

5.3.2.1 General

The following sequence of activities shall be applied to identified hazards, hazardous conditions, and functions whose failures have hazardous consequences:

1. Hazard elimination
2. Hazard minimization
3. Hazard control.

5.3.2.2 Hazard elimination

Hazards and hazardous conditions shall, consistently with the project constraints and objectives, be eliminated from the design and operational concepts by the selection of design technology, architecture and operational characteristics.

5.3.2.3 Hazard minimization

Where hazards and hazardous conditions are not eliminated, the severity of the associated hazardous events and consequences shall, consistently with the project constraints and objectives, be reduced to an accepted level through the change of the design architecture, technologies, and operational characteristics allowing the substitution of those hazards by other hazards with lower potential threat.

5.3.2.4 Hazard control

5.3.2.4.1 General

Hazards that have not been eliminated and have been subjected to hazard minimization (as defined in 5.3.2.3) shall be controlled through preventive mitigation measures, associated to hazard scenarios, which are introduced into the system design and operation to avoid the events or to interrupt their propagation to consequences.

The following measures shall be applied in order of precedence:

1. Design selection
2. Automatic safety devices
3. Warning devices
4. Special procedures

5.3.2.4.2 Design selection - Failure tolerance design

Failure tolerance is the basic safety requirement that shall be used to control most hazards.

The design shall tolerate a minimum number of credible failures and/or operator errors determined by the hazard consequence.

Each SST partner shall establish the list of failures to be considered as “non credible” (i.e. very unlikely) for SST-PRO approval as early as possible in development.

5.3.2.4.3 Design selection - Design for minimum risk

Hazards which cannot be controlled by compliance to failure tolerance shall be reduced to an accepted level by compliance with specific safety-related properties and characteristics of the design.

5.3.2.4.4 Automatic safety devices

Hazards that are not eliminated through design selection shall be reduced and made controllable through the use of automatic safety devices as part of the system, subsystem or equipment.

5.3.2.4.5 Warning devices

When it is not practical to preclude the existence or occurrence of known hazards or to use automatic safety devices, devices shall be used for the timely detection of the hazardous condition and the generation of a warning signal.

This shall be coupled with emergency controls of corrective action for operators to safe or shut down the affected subsystem.

5.3.2.4.6 Special procedures

When it is not possible to reduce the magnitude of a hazard through the design, the use of safety devices or the use of warning devices, special procedures shall be developed to control the hazardous conditions for the enhancement of safety.

Special procedures shall be verified by test and appropriate training shall be provided for personnel.

Hazard detection shall be implemented if alternative means cannot be used.

To permit the use of real-time monitoring, hazard detection and safing[3] systems for hazard control, the availability of sufficient response time shall be verified and corresponding safing procedures shall be developed and verified and the personnel trained.

5.3.3 Environmental compatibility

The system design shall meet the safety requirements under the worst-case natural and induced environments defined for the project, as defined in the Telescope Technical Requirements Specification [AD01].

Design and performance margins shall be established and applied for worst-case combinations of induced and natural environments and operating characteristics.

5.3.4 External services

Loss, malfunctioning, and sudden restoration of external services shall be defined as an input to the development phase.

The system design shall be defined so that catastrophic or critical consequences are not induced by loss, malfunctioning, and sudden restoration of external services.

5.3.5 Hazard detection - signalling and safety

Safety monitoring, display, alarm and safing capabilities shall be incorporated.

These capabilities shall provide the information to allow the system operators to take actions to protect personnel from the consequences of failures within safety-critical functions and the failure of hazard control measures.

The system design shall provide the capability for detecting failures that result in degradation of failure tolerance with respect to the hazard detection, signalling and safety function.

The performance of these functions shall be verifiable during operational phases.

[3] Safing: the process of making safe through a dedicated system or function

The emergency, caution and warning function shall detect and notify the system operators of emergency, warning and caution situations.

Safety functions and capabilities, which provide for the containment or control of emergency, warning and caution situations, shall be included.

Provisions shall be included for the monitoring of safing function execution.

Dedicated safing functions shall be provided for emergency situations.

A single failure shall not cause loss of the emergency and warning function.

Where the operation of a safety system introduces a new hazard, inadvertent activation of the safety system shall be controlled in accordance with the failure tolerance requirements.

A single failure shall not cause loss of the emergency and warning functions together with the monitored functions.

Emergency, warning and caution data, out of limit annunciation and safety commands shall be given priority over other data processing and command functions.

5.3.6 Access

System shall be designed such that any required access to system elements during operations can be accomplished with an accepted level of risk to personnel.

5.4 Safety risk reduction and control

5.4.1 Severity of hazardous event

The severity of potential consequences of identified hazardous events shall be categorized as shown in Table 5-1.

Severity	Level	Dependability	Safety
Catastrophic	1	Failures propagation	Loss of life, life-threatening or permanently disabling injury or occupational illness; Severe detrimental environmental effects. Loss of site facilities; System loss (unrecoverable at reasonable cost or more than 4 weeks out of operation)
Critical	2	Loss of system	Temporarily disabling but not life-threatening injury, or temporary occupational illness; Major damage to site facilities; Major detrimental environmental effects. (repairable but support necessary and/or up to 4 weeks out of operation)
Major	3	Major system degradation	Minor damage to site facilities;

			Minor detrimental environmental effects. (repairable by CTAO up to 1 week out of operation)
Minor or negligible	4	Minor system degradation or any other effect	Less than minor injury, less than occupational illness (irritation) Minor system damage (less than 1 day out of operation)

Table 5-1: Severity of consequences

Detrimental environmental effects, from the point of view of severe hazardous consequences to the global public, shall be included in the consequence severity evaluation.

5.4.2 Failure tolerance requirements

5.4.2.1 Basic requirements

Failure tolerance shall be the basic safety requirement used to control hazards.

No single system failure or single operator error shall have critical or catastrophic consequences.

Safety inhibits shall be independent, verifiable, stable and stay in a safe position even in case of energy failure.

Multiple failures, which result from common-cause or common-mode failure mechanisms, shall be analysed as single failures for determining failure tolerance.

5.4.2.2 Failure propagation

Hardware failures or software errors shall not cause additional failures with hazardous effects or propagate to cause the hazardous operation of interfacing hardware.

5.4.3 Design for minimum risk

5.4.3.1 General

“Design for minimum risk” is a safety requirement used to control hazards by specifying safety-related properties and characteristics of the design.

Technical requirements for areas of design for minimum risk shall be identified and approved by the relevant safety approval authorities.

5.4.3.2 Safety factors

Structural safety factors shall be defined and applied.

Safety margins shall be based on worst credible combinations of environmental conditions.

5.4.3.3 Materials

Material selection shall assure that hazards associated with material characteristics are either eliminated or controlled. Examples of these material properties to be characterized are: toxicity, flammability, resistance to stress corrosion, outgassing, off gassing, resistance to thermal cycling, thermal degradation, resistance to cleaning fluid and microbiological growth. If this requirement cannot

be met, the system design shall include the necessary provisions to control hazardous events associated with material characteristics. An example of provisions to be included by the system design is containment of hazardous substances.

5.5 Identification and control of safety-critical functions

5.5.1 Identification

A function that, if lost or degraded, or through incorrect or inadvertent operation, can result in a catastrophic or critical hazardous consequence, shall be identified as a “safety-critical function”.

Identification shall be done without considering hazard controls to be or already implemented.

5.5.2 Status information

The system shall provide failure tolerance status information of safety-critical functions.

5.5.3 Safe shutdown requirements

The design shall provide the capability for the safe shutdown of safety-critical functions prior to maintenance operations.

5.5.4 Software functions

5.5.4.1 Software criticality

Safety aspects associated with the software function shall be an integral part of the overall system safety efforts and not be assessed in isolation.

A software component shall be considered safety-critical if the loss or degradation of its function, or its incorrect or inadvertent operation, can result in catastrophic or critical consequences.

5.5.4.2 Analysis of safety-critical software

During the project life cycle, safety analysis shall be carried out to:

1) identify the criticality of software components in accordance with the severity of the consequences, as defined in Table 5-1
2) determine where and under what conditions the system can trigger hazardous events caused by the software
3) define verification methods for hazard controls involving software
4) provide verification evidence of hazard control implementation.

5.5.4.3 Evaluation of software criticality

The criticality of a software component shall be evaluated taking into account the overall system design, which can provide for, e.g. back-up or emergency procedures, hardware inhibits and certain time to effect.

5.5.4.4 Software development

Safety-critical software shall be analysed for the identification and verification of adequate software controls and inhibits and validated accordingly.

The level of required software product assurance effort shall be determined in accordance with the criticality of the software component.

5.6 Operational Safety

5.6.1 Basic requirements

Safety involvement in the operational phase shall be planned.

Responsibilities, rules and contingency procedures shall be established prior to operation for hazardous "limit" conditions that can occur during operations.

Operating ranges and performance limits for safe operation shall be established and specified.

The design shall not require continuous active control by personnel in order to stay within the established operating ranges and performance limits.

Man-machine interfaces shall be designed and the personnel tasks shall be scoped to reduce the potential for hazardous events resulting from human error to an accepted level.

5.6.2 Operations

5.6.2.1 Applicability

Safety requirements shall be applied during the following operations:

1. development, qualification or acceptance testing;
2. assembly, integration or test operations;
3. observing operations;
4. maintenance operations;
5. transportation or handling operations.

5.6.2.2 Initiation

Each SST projects and contractor shall establish procedures to perform inspections prior to the performance of any applicable operation.

5.6.2.3 Review and inspection

To verify conformance to safety requirements, readiness reviews and inspections shall include safety review and assessment of facilities, equipment, test articles, operating, test and contingency procedures, access controls, and personnel capabilities to comply with the safety requirements.

5.6.2.4 Hazardous operations

Hazardous operations shall be monitored for conforming to safety requirements and procedures, and for the possible development of unforeseen hazardous situations.

The safety manager or safety relevant authority shall have the authority to stop any operation that does not conform to safety requirements.

6 Safety analysis requirements and techniques

6.1 Overview

Safety risks are the result of the hazardous characteristics associated with the:

- design, including the technology selected, the physical arrangement of elements, subsystems and equipment;
- operating modes;
- potential for operator error;
- operating environment;
- hazardous effects that result from the failure of functions (including software).

6.2 General

Safety analysis shall be performed in a systematic manner as a basis for all applicable phases and to ensure that hazards are identified, eliminated or minimized and controlled and safety risks are assessed and reduced.

Safety analyses shall be initiated early in the design process and provide concurrent support to project engineering in the selection of the least hazardous design and operational options that are compatible with the project constraints and conform to the requirements.

The results of safety analyses shall also be used to support project management in the assessment of the overall risks, verification of risk reduction, ranking of risk sources, support to project resource allocation, monitoring of risk trends, and residual risk acceptance.

6.3 Assessment and allocation of requirements

6.3.1 Safety requirements

Each SST project and contractor hall respond to and comply with applicable safety requirements

for the project.

6.3.2 Additional safety requirements

Each SST partner shall identify additional safety requirements, where applicable, through the use of lessons learned from previous projects and the safety analyses performed during the project.

6.3.3 Define safety requirements - functions

Each SST partner shall define the safety requirements for the various functions of the system.

6.3.4 Define safety requirements - subsystems

Each SST partner shall define the safety requirements associated with the various subsystems and lower levels.

6.3.5 Justification

Each SST partner shall justify the proposed allocation of safety requirements at the latest at the end of the detailed definition phase.

6.3.6 Functional and subsystem specification

Each SST partner shall ensure that the function and subsystem safety requirements are included in the relevant functional and subsystem specification.

6.4 Safety analyses during the project life cycle

Safety analysis shall be refined and updated in an iterative manner as the design process proceeds, to ensure that hazards and hazardous events are assessed, and that the relevant detailed design and operational requirements, hazard controls, and verification activities are defined and implemented.

6.5 Safety analyses

6.5.1 Safety Analysis Requirements

The safety analysis requirements are defined in the applicable EU Directives, e.g. Machinery Directive 2006/42/EC.

Not only the individual telescopes and other similar products are covered by the Machinery Directive, also the entire SST Array of CTA-South is considered as a machine.

6.5.2 Safety Analysis Techniques

If the applicable EU Directives do not specify different processes, the analysis techniques defined in the [RD12] shall be used for the preparation of the safety assessment documents.

6.5.3 Hazard analysis

Hazard analysis shall be performed in a systematic manner, beginning in the concept phase and continuing through the operational phase, including end-of-life and disposal.

Hazard analysis shall support the hazard reduction process.

Hazard analysis shall identify and evaluate:

1) hazards associated with system design, its operation, and the operation environment;

2) the hazardous effects resulting from the physical and functional propagation of initiator events;
3) the hazardous events resulting from the failure of system functions and functional components;
4) time critical situations.

The following potential initiator events shall be considered:

1) hardware failure (random or time dependent);
2) latent software error;
3) operator error;
4) design inadequacies, including:
   a) inadequate margins;
   b) unintended operating modes caused by sneak-circuits;
   c) material inadequacies and incompatibilities;
   d) hardware-software interactions;
5) natural and induced environmental effects;
6) procedural deficiencies.

Hazard analysis includes a systematic analysis of the "system" operations and operating procedures that shall be performed in the detailed design and operational phases of the project.

This analysis evaluates the capability of the system to be operated safely, to determine the safest operating modes, and to evaluate the acceptability of the operating procedures.

The systematic analysis of system operation and operating procedures shall be repeated as the design and operation details evolve, including the system's operational modes and man-machine interfaces.

6.5.4 Safety risk assessment

Safety risk assessment shall:

1) comprise the identification, classification and ranking of safety risks and their contributors,
2) be based on deterministic hazard analysis by combining the consequence severity and the likelihood of occurrence;
3) be used to facilitate effective and efficient safety risk reduction and control;
4) support project risk management;
5) assess compliance with probabilistic safety targets.

The estimation of event likelihoods is based on the use of different sources of data i.e.:

- Previous experience on the particular system (i.e. measured or directly observed relevant test or experience data),
- Data from other system or projects (i.e. extrapolation from generic data, similarity data, or physical models),
- expert judgment (i.e. direct estimation of likelihoods by domain specialists).

The determination of likelihood is not a mean to downgrade the severity of function.

Safety risk assessment shall be started early in the design process and performed in progressive steps during the implementation of the safety programme.

6.5.5 Supporting assessment and analysis

6.5.5.1 Warning time analysis

Warning time analysis shall be performed during the concept definition phase and the design and development phase in order to evaluate time-critical situations identified in the hazard analysis and to support the implementation of hazardous-situation detection and warning devices or contingency procedures.

The analysis shall determine the:

1) time interval during which the event is detected and the response action taken;
2) detection capability of the proposed design with respect to detection sensitivity and detection time;
3) resultant time available for response;
4) adequacy of the proposed design or contingency procedures, including system reconfiguration and maintenance.

The detection times shall be determined from the:

1) occurrence of the initiating event to the time when a hazardous consequence occurs (propagation time)
2) occurrence of the initiating event to the time of earliest detection or annunciation;
3) time taken for corrective action to be implemented.

6.5.5.2 Common-cause and common-mode failure analysis

6.5.5.2.1 Multiple failures

Multiple failures, which result from common-cause or common-mode failure mechanisms, shall be analysed as single failures for determining failure tolerance.

6.5.5.2.2 Identification of requirements and scope

Each SST project and contractor shall identify the requirements for and the scope of dedicated common-cause and common-mode analyses by means of the review of the results of the other safety analyses, such as fault-tree analysis and hazard analysis, and of the characteristics of the system and of its environment.

6.5.5.2.3 Identification of common-cause failures

The SST partner shall identify potential common-cause failures by assessment of the effects of common-causes.

The common-cause failure analysis shall be performed in coordination with the fault-tree analysis and the hazard analysis.

6.5.5.2.4 Analysis of common-mode failures

Common-mode failures shall be analysed by means of the use of check-lists (to be established by the SST partner) that list potential common-modes for system components during the manufacturing, integration, test, operation and maintenance phases.

The common-mode analysis shall be coordinated with the FMEA/FMECA (6.5.5.5).

6.5.5.2.5 Integration of results

Results of common-cause and common-mode analysis shall be integrated with the results of the system level safety analyses (fault tree analysis, hazard analysis).

6.5.5.3 Fault tree analysis

The fault tree analysis shall be used to establish the systematic link between the system-level hazard and the contributing hazardous events and subsystem, equipment or piece part failure.

A fault tree analysis, or its equivalent, shall be performed to verify the failure tolerance requirements.

6.5.5.4 Human error analysis

Whenever safety analyses identify operator errors as a cause of catastrophic or critical hazards, a dedicated analysis shall be carried out.

The human error analysis shall be used to support the safety analysis for the identification of human operator error modes and their effects and for the definition of adequate countermeasures to prevent or control human operator errors.

The human error analysis shall be developed from the early phases of the project onwards in order to define recommendations for the hardware and software design, procedure development and training preparation programme.

6.5.5.5 Failure modes, effects and criticality analysis

The results of failure modes and effects analysis (FMEA) or failure modes, effects and criticality analysis (FMECA) shall be used to support the hazard analysis in the evaluation of the effects of failures. FMEA/FMECA and hazard analysis are complementary analyses.

7 Safety Verification

7.1 General

A system shall be in place that tracks all hazards and related risks, to relate all verifications of the corresponding hazard uniquely to unambiguous causes and controls.

To successfully complete the safety process, positive feedback shall be provided on completion results for all verification items associated with a given hazard.

For all safety verifications, traceability shall be provided by means of implementation and execution of the following subsections.

7.2 Hazard Reporting and Tracking System

A centralized Hazard Tracking System (HTS) will be installed by the Safety Manager at his/her Project Office in order to systematically register all hazards at all project levels with potentially catastrophic or critical consequences.

All critical and catastrophic hazards identified during Manufacturing, Integration, Assembly and Verification (MAIV) shall be reported immediately after detection in writing to the Safety Manager. Those identified analytically during the preparation of the hazard analyses shall be specifically marked and listed in a dedicated section of the hazard analyses.

Together with the reporting of the critical and catastrophic hazards, each SST Institute or Contractor shall provide evidence that:

1. hazard controls methods are defined and agreed by the Safety Manager,
2. the verification methods are defined and agreed by the Safety Manager,
3. the verification is systematically completed.

The status of the identified critical and catastrophic hazard risk reduction activities shall be documented and reported to the relevant Project Manager by the Safety Manager.

7.3 Safety status review

The status of the hazard control and risk reduction activities shall be reviewed at Programme progress meetings and phase related design reviews (PDR, CDR, etc.) for compliance with decisions taken and achievement of intended results.

7.4 Safety verification methods

A systematic safety verification approach shall be implemented on all SST items. This approach shall start from the beginning of the preliminary design phase and shall continue through all project phases. As a minimum, the activities of the following two subsections plus those verification activities required by the national safety legislation shall be included.

7.4.1 Verification engineering and planning

Verification engineering shall select the verification methods consistent with the verification requirements.

Verification planning shall commence in an integrated manner upon selection of the control method.

7.4.2 Methods and reports

Safety verification methods shall include (alternatively or in combination) review of design, analysis, inspection and test.

For all safety verifications traceability shall be provided.

7.4.3 Analysis

All relevant technical safety and engineering analyses performed or updated in respect to the as-built configuration shall be used for verification.

When similarity analysis is provided, for tracking purposes it shall contain a copy of (or a unique reference to) the referenced previous verification, verification procedure and requirement valid at the time of the first verification.

7.4.4 Verification and approval

The SST partner shall select, and propose to the safety approval authority, the safety verification methods to be used in conformance to the applicable safety requirements.

The results of safety verification shall be submitted for approval to the relevant safety approval authority.

7.4.5 Safety Compliance Assessments

The following Table 7-1 describes the safety compliance assessment activities to be performed during the individual project phases:

Project phase					
Task number	Activity title	Preliminary design	Final design	Production &AIT/V	Operation
1	Identification of essential safety requirements				
1a	Preparation of Preliminary Hazard List (PHL)	A	AC	AC	AC
1b	Preparation of Preliminary Hazard Analysis (PHA)	A	NA	NA	NA
1c	Preparation of the	A	AC	AC	AC

	List of Relevant Provisions				
2	Performing a Conformity Assessment Cycle				
2a	Preparation of Hazard Analysis (HA)	NA	A	AC	AC
2b	Preparation of the Technical File	NA	A	A	A
2c	Preparation of Declaration of Conformity/Incorporation	A	A	A	A
3	Conformity Marking	A	A	A	A

Table 7-1: Safety Compliance Assessment Activities.[4]

7.4.6 System Safety Compliance Assessments

At the beginning of the individual project phases, and in the absence of the subsystem safety compliance assessment results, the preparation of the system safety compliance assessments will start on the assumption that all subsystems completely fulfil all essential safety requirements defined in the relevant EU Directive. The system safety compliance assessments will be revised as soon as the results of subsystem safety compliance assessments become available during the individual project phases.

7.4.7 Subsystem Safety Compliance Assessments

The SST Institutes and Contractors are responsible for the execution of the tasks on product level. The resulting documents defined by the EU directives and the associated harmonized standards are part of the product design review documentation and the preparation effort shall be reported in the standard progress reports and progress meetings. The results of the product activities shall be provided during the individual project phases early enough to enable their incorporation into the system level activities.

7.4.8 Safety Inspections and Tests

Safety critical functions shall be inspected and tested by the contributor during MAIV phase and the subsequent project phases.

Inspections and tests which are considered as necessary in order to meet safety requirements of the system shall be identified and included in

1. the MAIV procedures,
2. the installation and commissioning plans and procedures,
3. the operation manuals and procedures.

[4] A = applicable; AC = applicable to changes; NA = not applicable

7.5 Verification of safety-critical functions

7.5.1 Validation

Safety-critical functions shall be verified by testing, which includes application of the operating procedures and verification of the effectiveness of applicable failure tolerance requirements.

The tests shall include the demonstration of nominal, contingency and emergency operational modes.

7.5.2 Qualification

The safety-critical characteristics of all safety-critical functions shall be qualified by test.

Safety-critical function qualification testing shall include the determination of performance margins considering worst case combinations of induced and natural environments and operating conditions.

Qualification “by similarity” shall not be applied except after SST-PRO approval on a case-by-case basis.

7.5.3 Failure tests

Induced failure tests shall be performed when required by safety analysis for evaluating failure effects, and for demonstrating failure tolerance conformance in safety-critical functions.

7.5.4 Verification of design or operational characteristics

Verification of unique safety required design or operational characteristics shall form part of the development, qualification or acceptance testing programme as appropriate.

7.6 Hazard close-out

7.6.1 Safety assurance verification

In time for acceptance by the SST-PRO, and in preparation of transfer to the next stage of system integration, the safety manager shall verify that:

1. hazard close-outs performed so far by the responsible engineer are still valid;
2. the verifications reflect the as-built or as-modified status of the hardware;
3. all open verifications at this time are acceptable for transfer to the next stage of system integration

7.6.2 Hazard close-out verification

The safety manager shall ensure that each hazard considered for closure has the approval by the safety approval authority, verifying that

1. hazards not eliminated are controlled in accordance with the applicable requirements and associated verification activities are successfully completed, or, when applicable,
2. deviations from, or waivers of, requirements are granted by the safety approval authority.

7.7 Declaration of conformity

The Declaration of conformity shall be done in accordance with the Machinery Directive 2006/42/EC, the EMC Directive 2014/30/EC, the LVD Directive 2014/35/EU, and other applicable EU Directives.

Definition:

The EC declaration of conformity is the written statement reporting a single declaration drawn up by the manufacturer to demonstrate the fulfilment of the essential EU safety requirements relating to a product bearing the CE marking it has manufactured.

End of the document