Telescope Safety Design Specification

Doc. No: CTA-SPE-TEL-000000-0003_1a

2023-01-18

	First/Last Name, Organisation, Role	Digital signature
Prepared by (1)	Stefano Stanghellini CTAO Telescope Coordinator	
Prepared by (2)	Amaya Paredes CTAO Telescope Engineer	
Approved by (1)	Nick Whyborn CTAO Lead System Engineering	
Approved by (2)	Karl Tegel CTAO Safety Engineer	
Released by	Wolfgang Wild CTAO Project Manager	

Revision History				
Issue	**Rev.**	**Created**	**Reasons / Remarks / Section**	**Author**
1	a	2023-01-18	New issue	S. Stanghellini

Authors	
First/Last Name, Organisation	**Contribution Subject/Chapter**
S. Stanghellini, CTAO	All Chapters
A. Paredes, CTAO	Various contribution
A. van Kesteren , ESO	Comments on initial version
K. Tegel, CTAO	Review, standards

Definitions	
Shall	*Shall means “mandatory”*
Telescope	*Telescope indicates Telescope structure and Camera*

Table of Contents

Index of Tables

1 Purpose and Scope

This document summarizes the most common requirements associated to the safe design of the telescope in accordance with the Directive 2006/42/EC on machinery [AD01]. The requirements herein are generally implemented in optical and radio telescopes but have been adapted to Cherenkov telescopes. This specification does not pretend to cover all safety aspects, which may apply in various fields of the Cherenkov telescopes like electrical safety, power distribution and others, which are in general covered by applicable norms and standards. It covers much more the design aspects which are linked to a safe operation and protection of telescopes.

The variety of the different type of design of the telescopes of CTAO (up to four different structure and five cameras) makes certain safety design features not applicable to all individual Cherenkov telescopes. In general, it is expected that the spirit and the objectives of the requirements herein listed are fulfilled by the various CTAO telescope designs, whereby deviations from the specific implementation can be considered and accepted by the CTAO project, under specific review based on hazard analysis and/or a change request process.

1.1 Applicable Documents

The following documents are integral part of this specification within their limits:

AD #	Title
AD01	Directive 2006/42/EC of the European Parliament (on machinery) MD
AD02	IEC 62061:2021, Safety of machinery – Functional safety of safety-related electrical electronic and programmable electronic control system
AD03	IEC/TR 62061-1:2010 Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
AD04	CTA-PLA-SEI-00000-0001 CTA Product Safety Plan
AD05	EN ISO 13849-1:2015-Safety of Machinery – Safety related parts of Control Systems - General principles for design.
AD06	EN-ISO 12100:2010 – Safety of Machinery General principles of Design - Risk assessment and risk reduction
AD07	CTA-TEL-SPE-000000-002_01c Telescope Grounding - lightning and LEMP Protection
AD08	CTAO Structural Design and verification Guidelines *(to be released)*
AD09	EN IEC 60332-3, Tests on electric cables under fire conditions - Part 3-22: Test for vertical flame spread of vertically-mounted bunched wires or cables - Category A
AD10	Directive 2014/35/EU (Low Voltage)
AD11	Directive 2014/30/EU (EMC)
AD12	EN ISO 14122:2016 Safety of Machinery Permanent means of access to machinery

AD #	Title
AD13	EN ISO 13850:2015 Safety of Machinery Emergency Stop -Principles of design
AD14	EN 60204-1:2016 Safety of machinery – Electrical equipment of machines – Part 1: General requirements
AD15	EN 60364: Low-voltages electrical installations – Part 1 (IEC 60364-1:2005), Part 4-41 (IEC 60364-4-41:2017), Part 4-42 (IEC 60364-4-42:2014), Part 4-43 (IEC 60364-4-43:2008), Part 4-44 (IEC 60364-4-44:2018), Part 5-52 (IEC 60364-5-52:2009), Part 5-53 (IEC 60364-5-53:2020), Part 5-54 (IEC 60364-5-54:2011), Part 5-56 (IEC 60364-5-56:2018), Part 6(IEC 60364-6:2016)
AD16	EN ISO 4413: 2010 Hydraulic fluid power — General rules and safety requirements for systems and their components
AD17	EN 60445:2017 Basic and safety principles for man-machine interface, marking and identification - Identification of equipment terminals, conductor terminations and conductors
AD18	EN 61000 Electromagnetic Compatibility (EMC)- Part 1-1 (IEC TR 61000-1-1:1992), Part 1-2 (IEC 61000-1-2:2016), Part 2-4 (IEC 61000-2-4:2002), Part 2-5 (IEC TR 61000-2-5:2017), Part 5-2 (IEC TR 61000-5-2: 1997).
AD19	EN ISO 4414:2010 Pneumatic fluid power — General rules and safety requirements for systems and their components
AD20	IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General requirements
AD21	IEC TR 61508-0:2005 Functional safety of electrical/electronic/ programmable electronic safety related systems – Part 0: Functional safety and IEC 61508
AD22	ISO/IEC 17050-1:2004 Conformity assessment — Supplier's declaration of conformity — Part 1: General requirements
AD23	Directive 2011/65/EU (RoHS Directive)
AD24	Directive 2015/863/EU (amending Annex II to Directive 2011/65/EU of the European Parliament and of the Council as regards the list of restricted substances)
AD25	IEC 61025:2006 Fault tree analysis (FTA)

1.2 Reference Documents

RD #	Title
RD01	Occupational Safety and Health Administration – OSHA Regulations (Standards - 29 CFR). PART 1910 Occupational Safety and Health Standards PART 1926 Safety and Health Regulations for Construction
RD02	Directive 2001/95/EC, of 3 December 2001 on general product safety

RD #	Title
RD03	Directive 2009/104/EC of 16th September 2009 - Minimum safety and health requirements for the use of work equipment by workers at work
RD04	Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH)

1.3 Abbreviations and Acronyms

Abbreviation	Definition
ACADA	Array Control and Data Acquisition
AC	Alternating Current
AD	Applicable Document
CDMR	Critical Design and Manufacturing Readiness Review
CDR	Critical Design Review
CTA	Cherenkov Telescope Array
CTAO	Cherenkov Telescope Array Observatory
DC	Direct Current
DoC	Declaration of Conformity
DoI	Declaration of Incorporation
DRD	Document Requirement Definition
EHSR	Essential Health and Safety Requirements
EMC	Environmental Compatibility
ESO	European Southern Observatory
ESS	Emergency Stop System
FMECA	Failure Mode Effect and Criticality Analysis
FTA	Fault Tree Analysis
HA	Hazard Analysis
HAZMAT	Hazardous Materials
HML	Hazardous Materials List
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
PBC	Protective Bonding Circuit

Abbreviation	Definition
PELV	Protective Extra Low Voltage
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour.
PL	Performance Level
PLC	Programmable Logic Controller
PPE	Personal Protection Equipment
RoHS	Restriction of Certain Hazardous Substances
SELV	Safety Extra Low Voltage
SIL	Safety Integrity Level
SRCF	Safety Related Control Function
SRS	Safety Requirements Specification
TBD	To Be Defined
TRR	Test Readiness Review

2 General Safety Technical Specification

2.1 General

The telescope and their subsystems shall conform to the requirements given in the Essential Health and Safety Requirements (EHSR) given in its Annex 1 of [AD01] and the harmonized European standards. The conformity shall apply under all lifecycles (assembly, disassembly, testing, storage, integration, verification, operation, maintenance, power off, etc.), including all applicable environmental factors.

The Directive 2001/95/EC [RD02] on general product safety, also known as the General Product Safety Directive (GPSD), requires manufacturers of machinery to ensure, that products placed on the marked are safe to use and cause no harm. A product is considered safe when it meets specific national requirements or EU harmonizes standards. By using the EU harmonized standards, the presumption of conformity is given, if national standards are used, the conformity must be proven by a notified and certified body.

Safe design compliance with these EHSRs shall be verified using harmonised standards that are listed in the most recent Official Journal of the EU and that are applicable to the (sub)system called in the Chapter 1.1 (Applicable Documents) and their associated standards.

Conformance to the requirements of the Machinery Directive shall be shown by means of a Hazard Analysis and full related documentation.

Subsystems presenting a safety risk as indicated by the Hazard Analysis shall be evaluated and risk mitigation measures shall be implemented to reduce the risk to an acceptable level.

Fire prevention must also be considered – as relevant - in the Hazard analysis and comply with local legal regulations.

In accordance with the directive 2006/42/EC on machinery [AD01], the safety precautions shall consider in descending order of priority:

a. protection of persons,
b. protection of environment,
c. protection of equipment.

2.2 Designing for Safety

Following the hazard analysis and risk assessment, risk reduction measures shall be proposed. These risk reduction measures shall be divided into the following four levels:

1. *Safe design (non-functional safety)*

These measures shall take top priority within the scope of risk reduction. To ensure a safe design complying with the EHSRs of all applicable EU Directives, the appropriate harmonized EN standards that are applicable to the (sub)system shall be followed.

Examples (not exhaustive):

- Mechanical design (e.g. avoidance of sharp edges, avoidance of crushing, shearing and entanglement points).
- Electrical design (e.g. protection against electric shock, overcurrent protection, control, shut down, mains connection, EMC).
- Equipment involving gas, fluids (e.g. pressure control, leaks, acoustic attenuation). Evaluation of possible substitution for low hazard and low toxicity gas and fluids.
- Concepts for operation and maintenance (maintainability, reliable and available components, ergonomic principles for handling).

2. Technical Protective Measures (functional safety)

A safety function, also called interlock, must be defined for each hazard which can't be eliminated by means of design measures in subsystems of the telescope structure. Several of such safety functions may be needed in the telescope to achieve an acceptable risk level. For the purpose of risk reduction, a SIL analysis in according to [AD02][1] and/or PL level according to [AD05] shall be defined and verified for each safety function.

The IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 1: General Requirements [AD20], covers those aspects to be considered when electrical/electronic/programmable electronic systems are used to carry out safety functions. The documentation shall contain sufficient information, for each phase of the overall system and software safety lifecycles completed, necessary for effective performance of subsequent phases and verification activities.

The IEC TR 61508-0:2005 Functional safety of electrical/electronic/programmable electronic safety-related systems Part 0: Functional safety and IEC 61508 [AD21], introduces the concept of functional safety and gives an overview of the IEC 61508 series.

3. User required organisational and/or procedural measures of remediation

Procedures and measures needed to reduce residual risks shall be proposed to CTAO, as part of the design for safety and safety evaluation, and shall be later covered in manuals and procedures.

4. Information and training on operation, residual risks and protective equipment

Operation and maintenance staff must be informed on possible residual risks and on requirements on personal protective equipment (PPE). This information does not replace the requirements of safe design and technical protective measures. It may include warnings, signage, training, instructions and similar.

2.3 Hazard Analysis

Hazard analysis is the process of recognizing hazards that may arise from a system or its environment, documenting their unwanted consequences and analysing their potential causes. The hazard analysis must:

[1] Refer to [AD03] for guidance on the application of IEC 62061 [AD02] in the design of safety-related control systems for machinery.

- Determine the risks associated with the hazardous events according to the principles mentioned in AD04.
- Determine the hazards and hazardous events of the equipment under control and the control system (in all modes of operation), for all reasonably foreseeable circumstances including fault conditions and human errors.
- Analyse the event sequences leading to the hazardous events identified, in the form of a Fault Tree Analysis (FTA)[2]
- Include if relevant, an assessment of hazards related to hazardous materials (HAZMAT) in the form of a HAZMAT list.
- The hazard analysis shall, after listing all possible hazards, include an assessment of their severity and probability of a hazard and perform the so-called risk assessment by using the hazard classification matrix and the proposed remedial measures.
- Hazards may be related to different operational states of the system. This includes (but is not necessarily limited to) operation, shutdown and maintenance (including handling procedures).

As the design of the system progresses the hazard analysis shall be kept up to date reflecting new considerations and design information and the risk assessment shall be re-evaluated as needed.

2.3.1 Hazard Severity

Hazard severity categories are defined to provide a qualitative measure of the hazard (both to systems and staff).

Category	Description	Definition
I	CATASTROPHIC	Potential fatality (death) System loss (unrecoverable at reasonable cost or more than 4 weeks out of operation)
II	CRITICAL	Severe injury, major occupational illness Major system damage (repairable but support necessary and/or up to 4 weeks out of operation)
III	MARGINAL	Minor injury, minor occupational illness Minor system damage (repairable by CTAO up to 1 week out of operation)
IV	NEGLIGIBLE	Less than minor injury, less than occupational illness (irritation) Minor system damage (less than 1 day out of operation)

Table 1 - Hazard Severity Categories

[2] Equivalent to FMECA. According to standard IEC 61025:2006 [AD25].

2.3.2 Hazard Probability

Classification of the probability of hazards occurring during the expected lifetime is defined in the following table:

Probability Levels			
Description	Level	Probability of occurrence	
		Qualitative description	Quantitative description/year
Frequent	A	Likely to occur often in the life of an item	$>10^{-1}$
Probable	B	Will occur sometime in the life of an item	10^{-2} - 10^{-1}
Occasional	C	Unlikely, but possible to occur in the life of an item	10^{-4} - 10^{-2}
Remote	D	Very unlikely to be expected in the life of an item	10^{-6} - 10^{-4}
Improbable	E	Extremely unlikely, so that it can be assumed occurrence may not be expected in the life of an item	$<10^{-6}$

Table 2 – Probability Levels

2.3.3 Hazard Risk Acceptability Matrix

The following matrix defines the degree of acceptability of the various hazard categories:

Risk	**Severity**			
	Catastrophic	**Critical**	**Marginal**	**Negligible**
Likelihood (per item per lifetime)	**I**	**II**	**III**	**IV**
Frequent (A)				
Probable (B)				
Occasional (C)				
Remote (D)				
Improbable (E)				

Table 3 – Hazard Risk Acceptability Matrix

Where:

Red (Unacceptable):	Serious risk above the limits tolerated by CTAO (IA, IIA, IIIA, IB, IIB, IIIB, IC, IIC)
Orange (Undesirable):	Considered as undesirable risk. It shall be lowered or only accepted after written approval by CTAO (ID, IIC, IVA)
Yellow (Acceptable with review):	Medium risk which can be considered acceptable after extensive evaluation (IE, IID, IVC)
Green (Acceptable) means:	Low risk within the limits accepted by CTAO (IVC, IIID, IVD, IIE, IIIE, IVE)

2.4 Specific Installations and Systems

2.4.1 Electrical Systems

Safety, electrical and electronic installations and equipment shall comply with the relevant requirements set in EN 60204-1 [AD14].

In case a system can be defined as 'machinery' one shall use EN 60204-1 [AD14] for its electrical equipment as a basis to presume compliance with the Machinery Directive [AD01] and Low Voltage Directive [AD10] plus any additional harmonized standards that may fall under the scope of the specific system. Refer to 2.4.1.1 for more details about the EU applicable directives.

As stated in AD04, components and equipment used on systems shall comply with their harmonized EN product or product-family standard or - in case this is not available - a generic standard. Commercially available equipment (COTS) shall bear the CE mark. In case suitable equipment with a CE mark is not available, the usage of non-CE marked equipment shall receive explicit approval by CTAO and shall be in compliance with the EHSRs of all applicable EU directives.

Custom made products shall be checked for compliance to the most appropriate harmonized standards under the scope of the applicable Directives. Directive 2011/65/EU [AD23] compliance is mandatory for all COTS equipment.

All power cables (AC or DC) and relevant connection terminals shall bear identification in full compliance with the requirements of EN 60445 [AD17].

2.4.1.1 EU Directives

CTAO projects will be comprised of a variety of equipment and systems that shall be designed in compliance with the Essential Health and Safety Requirements (EHSR) contained in the various applicable EU Directives. To judge which of the Directives apply to a certain system or equipment the scope of the Directive shall be consulted.

Below a non-exhaustive list of EU Directives is given applying to most of the equipment and systems developed for CTAO projects.

2.4.1.1.1 Machinery Directive

The Machinery Directive 2006/42/EC applies to machinery [AD01]. In its Annex 1 it specifies essential health and safety requirements (EHSR) that are to be complied with. Harmonized standards that fall under the scope of the Machinery Directive provide the means to presume compliance with the EHSR.

The Machinery Directive requires a hazard analysis / risk assessment to be completed for all products falling under its scope.

2.4.1.1.2 Low Voltage Directive

The Low Voltage Directive (LVD) 2014/35/EU [AD10] specifies EHSRs to ensure that electrical equipment within certain voltage limits provide an acceptable level of protection. The Directive covers electrical equipment designed for use with a voltage rating of between 50 and 1000 V for alternating current and between 75 and 1500 V for direct current referring to the voltage of the electrical input or output.

2.4.1.1.3 EMC Directive

The EMC Directive 2014/30/EU [AD11] states requirements to ensure that the electromagnetic disturbance generated by apparatus does not exceed a level allowing radio and telecommunications equipment and other apparatus to operate as intended, and that apparatus has an adequate level of intrinsic immunity to electromagnetic disturbance to enable it to operate as intended.

The EMC Directive applies to most electrical and electronic apparatus, that is, finished products and systems that include electrical and electronic equipment.

2.4.1.2 Protection against electric shock

2.4.1.2.1 General requirements

Protection of persons against electric shock from direct and indirect contact shall be achieved by:

1. *Protective measures for direct contact (also called 'protection under normal conditions'):*
   - Protection by enclosure
   - Protection by insulation of live parts
   - Protection against residual voltages
   - Protection by barriers (double/reinforced insulation)
   - Protection by placing out of reach or use of obstacles

2. *Protective measures for indirect contact (e.g. existing in case of a single fault condition):*
   - Prevention of the occurrence of a touch voltage
   - Protection by automatic disconnection of supply

3. *Use of protective or safety extra low voltage (PELV/SELV) where applicable*

The measures taken shall follow the requirements described in harmonized standards that are most applicable to the system or subsystem. For machinery the standard EN 60204-1 [AD14] shall be conformed to.

2.4.1.2.2 Protective bonding

Protective bonding is a basic provision for fault protection to enable protection of persons against electric shock from indirect contact. In each situation where protection against electric shock relies on a safe connection to earth, a systems metallic enclosure shall be earthed via the protective earth of

the power distribution. The protective bonding circuit (PBC) that is then formed, provides the return current path upon which the power distribution circuitry can react in case of a short circuit.

All requirements related to protective bonding shall be complied with, for this purpose EN 60364 [AD15] and EN 61000 (part 5-2 of AD18) are to be followed including possible additional requirements from applicable harmonized standard(s).

Protective bonding for machinery shall be compliant as per AD14 in general. In particular, it has to be compliant with 60364-4 and 60364-5 (parts 4 and 5 of AD15).

2.4.1.3 Telescope Grounding & Lightning Protection System

The requirements of AD07 and of the associated standards shall be adhered to.

2.4.2 Mechanical Structures

The safety of the mechanical structure shall be covered by adhering to AD08. This includes both serviceability limit state and ultimate limit state criteria. At the basis of the structural design there is the set of Eurocodes 0 - 4 (EN 1990 -EN 1994) and Eurocode 8 (EN 1998).

2.4.3 Hydraulic Systems

Any hydraulic system implemented in the telescope design shall be designed in accordance with AD16 (EN ISO 4413: 2010 Hydraulic fluid power — General rules and safety requirements for systems and their components).

2.4.4 Pneumatic Systems

Any pneumatic system implemented in the telescope design shall be designed in accordance with AD19 (ISO 4414:2010 Pneumatic fluid power — General rules and safety requirements for systems and their components).

2.4.5 Installations

For maintenance (both in-situ and/or off-situ), the design shall allow personnel to undertake work in a safe environment.

Pressure equipment and assemblies of pressure equipment shall be in conformance with the associated harmonized standards under the Machinery Directive [AD01].

All required pre-installations and personal implements for Personal Protective Equipment, and notably fall restraints for work in heights, shall be provided and shall be CE marked.

2.4.6 Confined Spaces & Lightning

Confined spaces in the sense of [RD01][3] where personnel are required to perform inspection or maintenance activities, shall be taken into account in the design with the associated required measures.

Amongst others, confined spaces shall be equipped with lights. Suitable lighting shall be provided to enable the safe work of personnel, and emergency lighting shall allow safe egress in all conditions.

Procedures related to confined spaces, including the use of manholes for access shall be established and covered in the maintenance manual.

Confined and/or lockable space shall be equipped with emergency possibility of opening from the internal side, in case of trapped personnel.

Confined space shall consider, if shown by the hazard analysis, alternate means of egress.

2.4.7 Access Ladders and Stairs

Stairs are preferred to ladders. If ladder access cannot be avoided, it shall be provided with adequate means of fall arrest. Fixed access ladders shall comply with part 4 of AD12 (EN ISO 14122-4:2016 Safety of Machinery Permanent means of access to machinery -Fixed ladders).

If ladders are used to access areas where specific maintenance interventions must take place, specific analyses shall be performed to show the safe bringing of maintenance tools to those areas.

2.4.8 Handling and Hoisting equipment

Handling equipment and hoist shall comply with all the applicable harmonised standards and be approved by certified institutions (TÜV, Bureau Veritas…).

Lifting equipment and hoist shall comply with harmonized standards under the Machinery Directive [AD01].

Handling equipment systems shall have adequate safety provisions to protect people and equipment from injuries or damage due to the movement of these systems. In particular, some of the safety functions (not necessarily a complete list) have been given a required minimum SIL or PL in Section 2.5.6.2 below.

Where deemed necessary or where demanded by the requirements of the Machinery Directive, handling equipment and systems shall be provided with acoustic and visual signals that alert people to the movement of these systems. These alert signals shall clearly identify the kind of warning involved and precede any movement.

2.5 Functional Safety

Functional safety refers to aspects of safety concerning the function of the system and involves the second step of the safety design process as explained above. If it is found during the hazard and risk

[3] OSHA uses the term "permit-required confined space" (permit space) to describe a confined space that has one or more of the following characteristics: contains or has the potential to contain a hazardous atmosphere; contains material that has the potential to engulf an entrant; has walls that converge inward or floors that slope downward and taper into a smaller areawhich could trap or asphyxiate an entrant; or contains any other recognized safety or health hazard, such as unguarded machinery, exposed live wires, or heat stress.

analysis of the system functions that a particular aspect results in an unacceptable or undesirable risk, specific risk must be mitigated or eliminated.

After analysing the (sub)system hazards and evaluating the need for risk reduction, functional safety is achieved when every allocated safety function is carried out at the level of performance (SIL or PL) required. The following steps are to be used:

I After analysing the (sub)system hazards and evaluation of the need for risk reduction, it shall be identified what the required safety functions are.

II Assignment of the risk-reduction required by the safety function in the form of a chosen SIL according to AD02 or PL according to AD05.

II The safety function shall be implemented by means of a safety related control system that is designed to represent the chosen SIL or PL taking into account the following:

- The architecture of the system.
- Reliability data for the constituent parts of the system.
- The Diagnostic Coverage representing the amount of fault monitoring in the system.
- Protection against common cause failure.
- Protection against systematic faults.
- Specific requirements for software.

It shall be ensured that the safety function performs according to the intended design, including under conditions of incorrect operator command and failure modes.

2.5.1 Interlocks

The telescope structure shall be provided with means to detect when an operating limit can be exceeded leading to a hazardous situation, an initiate an automatic control action. The hazardous situation shall be documented in the hazard analysis.

The resetting of an interlocking function shall not lead to initiation of hazardous machine operation.

Three categories of stop functions are defined in AD14:

- Stop category 0: stopping by immediate removal of power to the machine actuators.
- Stop category 1: a controlled stop with power available to the machine actuators to achieve the stop and then removal of power when the stop is achieved.
- Stop category 2: a controlled stop with power left available to the machine actuators.

In case of moving machinery an interlock shall lead to either a category 0, 1 or 2 stop in the definition of EN 60204-1 [AD14] as indicated by the risk assessment and the functional requirements of the machine.

Stop functions shall override associated start functions.

The implementation of an interlock function shall meet the Safety Integrity Level requirements depending on the probability of dangerous failures. The safety logic shall be implemented in safety-certified Programmable Logic Controllers (PLC). Appropriate sensors shall be selected to guarantee the demanded SIL level.

Interlock signals between failsafe PLCS and data transfer to and from remote I/O shall be transmitted by failsafe bus communication.

The status of each controller shall be available and monitored centrally.

Override

In case of trespassing operational limits an override of safeguards, is necessary to move out of the limits (ex. Az and elevation axes). In this case protection shall be ensured by the measures described in EN 60204-1 [AD14]:

- Disabling all other operating modes and one of the following:
  - Initiation by *Hold to Run* device.
  - Portable control station with emergency stop.
  - Wireless control station with stop and exclusive control.
- Limitation of speed or power of motion, and range.

This override function shall be such that the moving unit can be seen from the point where the override function is implemented.

2.5.2 Brakes

This section assumes as baseline that the structure has reversible axes. If this is not the case, modification of these requirements may be accepted under review. This can be the case, for instance, in the event gearboxes are implemented in the drive system.

Brakes shall be a of a safety break type (failsafe) with appropriate SIL level. The following applies:

- Brakes shall be able to prevent motion with nominal torque applied to the motors.
- Brakes shall be able to keep the structure in any position until the survival wind speed at the site[4].
- Brakes shall be engaged when no power is available.
- Brakes shall be equipped with a status signal.
- The time to release the brakes shall be less than 20 sec (command and execution)

2.5.3 Structure Axes limits

The altitude and azimuth axes movement ranges shall be limited outside the observing range by pre-limits, final limits, and end stops.

2.5.3.1 Software limits

Software limits, based on encoder readings shall be provided at the limit of the observing range, preventing commanding the telescope structure to go beyond the observing ranges.

2.5.3.2 Hardware limits

Unless covered by the Safety Integrity Level (SIL) provisions (see chapter 2.5.6), final limits and pre-limits based on hardwired limit switches shall be provided outside the observing range. Their positions will be chosen so as to stop the telescope structure before the final limit if it encounters the pre-limit

[4] This corresponds to 100 km/h for the CTAO-North site and 80 km/h for the CTAO-South site.

moving at its maximum velocity. The maximum velocity is assumed unless other methods with sufficient SIL level ensure that the speed is limited before reaching the pre-limit.

Specific implementation shall follow the requirements under section 2.5.1 above. Pre-limits and final limits shall have independent wiring, to avoid common mode failure.

When the pre-limit switch is actuated, the controller shall, in all operating modes, inhibit driving further in the same direction (into the limit), but should permit driving in the opposite direction (out of the limit). In this condition receipt of a command (either in remote or in a local control panel) that would cause motion into the limit shall cause the controller to enter fault state and thus to remove motor power and engage the brakes.

An override switch shall be provided to disable these features of the pre-limit switch. This switch shall be accessible only locally (not via remote control), and it shall not be on the control unit's front panel.

Note: the action of the pre-limit switch is not properly an interlock, being handled by the control system.

When the final limit switch is actuated, all motion of the structure shall be stopped by causing the controller to enter fault state immediately and remove power to the drives and engage the brakes. In addition, each final limit switch shall include a set of normally closed contacts through which at least one brake of its axis must be operated. There shall be no provision in the local control system for overriding the final limit switches. The designer shall include provisions for manual override of brakes and axis drives.

The position of the final limits shall be chosen so to prevent the structure to reach the end stops, if present, or any mechanical interference.

2.5.3.3 End stops

The hazard analysis shall be used to determine if altitude and/or azimuth energy absorbing end stops with shock absorbers shall be provided to protect all parts of the telescope structure as well as the equipment mounted on it (ex. Cherenkov camera) from damage if moving beyond the altitude and azimuth final limits.

Any energy absorbing end stops shall be based on passive systems. They shall be dimensioned in such a way to be able to protect the structure and its equipment from damage if the telescope structure travels into the end stop with maximum velocity or full motor torque. (These two events need not be considered simultaneously in the dimensioning of the end stops, as long as the hazard analysis has shown that sufficient safety is built into the system in order to prevent their simultaneous occurrence).

Similarly, if the end stops are not dimensioned for maximum velocity, it shall be shown by proper analysis what is the speed to be considered under consideration of the chosen SIL level.

The energy absorbing end stop must survive repeated use and have a lifetime of at least 15 years with nominal actuation of 3 times /year.

The energy absorbing system shall be chosen so that their performance is valid within the specified operational (observing) temperature ranges.

2.5.4 Locking pins/ locking system

As baseline the telescope structure shall be equipped with remotely operated motorized stow pins or analogous locking system for both azimuth and altitude axes in the parking position.

It shall be evaluated if:

- The locking system in azimuth associated to the parking position can make redundant the use of a locking pin.
- If a locking pin is needed when the telescope is not operational and not in parked position (example maintenance, access, or malfunction of the parking system).

Locking pins / system actuation shall not demand more than 30 sec.

At least two independent check methods, one software and one hardware, shall be available to guarantee the correct alignment of the locking pin (or any substitutive locking device), prior to enabling its insertion (actuation).

Status and fault detection shall be included in the system.

2.5.5 Emergency Stop

The telescope structure shall include an Emergency Stop System.

The telescope structure control system shall include an Emergency Stop System (ESS) on the structure axes. As a basic requirement the distribution and number of emergency stops shall allow action by the affected persons as well as witnesses at a distance.

The number of E-stop buttons and their location shall result from the hazard analysis and be approved by CTAO.

The E-Stop shall be a push-button operated switch, self-latching type and shall have positive opening operation according to AD13.

As covered by the standard, the actuator shall be colored red while the background immediately around the device actuator shall be colored yellow. The actuator shall be of the palm or mushroom head type.

It shall not be possible to restore the emergency stop device until it has been manually reset. Where several emergency stop devices are provided in a circuit, it shall not be possible to restore that circuit until all emergency stop devices that have been operated have been reset.

E-Stop shall be of category 1 (preferable, if allowed by risk analysis), or category 0. It shall be implemented with a safety integrity level (SIL) of 2 or higher. It shall follow the principal implementation requirements as stated in AD13.

It shall be evaluated if other movements beyond the structure main axes exists demanding the implementation of a category 1 emergency stop function (e.g. lifting devices or other mechanisms, shutter, but not the mirror position actuators…).

2.5.6 Safety Integrity Level

2.5.6.1 Introduction

A certain safety function is implemented by the safety-related parts of the machine control system to achieve or maintain the equipment under control in a safe state with respect to a specific hazard. A failure of the safety function can result in an immediate increase of the risks of using the equipment; that is, a hazardous condition. To reliably provide a specific safety function, it must continue to operate correctly under all foreseeable conditions.

EN IEC 62061:2021 [AD02], Requirements for the specification of Safety Related Control Functions (SRCFs), explains how the functional requirements specification and safety integrity requirements for each SRCF should be compiled to create a safety requirements specification (SRS). Furthermore, the three safety integrity levels (SIL1/2/3) require that the probability of dangerous failures per hour (PFH/PFD) must fall between certain target values as follows:

Low Demand Mode

SIL 1: $10^{-2} \leq PFD < 10^{-1}$ (or 1 failure in 10 years)

SIL 2: $10^{-3} \leq PFD < 10^{-2}$ (or 1 failure in 100 years)

SIL 3: $10^{-4} \leq PFD < 10^{-3}$ (or 1 failure in 1000 years)

High Demand Mode

SIL 1: $10^{-6} \leq PFH < 10^{-5}$ (or 1 failure in 100,000 h)

SIL 2: $10^{-7} \leq PFH < 10^{-6}$ (or 1 failure in 1,000,000 h)

SIL 3: $10^{-8} \leq PFH < 10^{-7}$ (or 1 failure in 10,000,000 h)

Based on that the safety related electrical control system shall be designed.

2.5.6.2 Required Safety Integrity Level

The chosen Safety Integrity Level (SIL) or Performance Level (PL) of the safety-related systems used in the telescope structure shall be of such a level to ensure that:

- the failure frequency of the safety-related systems is sufficiently low to prevent the hazardous event frequency exceeding that required to meet the tolerable risk and/or,
- the safety-related systems modify the consequences of failure to the extent required to meet the tolerable risk.

As baseline the minimum Safety Integrity Level (SIL) or Performance Level (PL) for the safety related systems implemented on the various subsystems shall comply with the following table:

Subsystem	Safety related control system	Minimum level	
		SIL	PL
Moving elements	Emergency Stop		
• Structure rotation axes • Others mechanisms (TBD)		2	d
• Lifting devices/hoist		2	d
Moving elements	End of travel detector		
• Structure rotation axes • Others mechanisms (TBD)		2	d
• Lifting devices/hoist		2	d
Moving elements:	(Over)speed detection		
• Structure rotation axes • Others mechanism (TBD)		2	d
Moving elements	Stop		
• Lifting device /hoist		1	c
Telescope structure	Locking Pin System (detection and actuation)		
• Azimuth axis • Altitude axis		2 2	d d
Lifting devices/hoist	Movement indication (visual, audible)	2	d
Fire protection (TBD) if applicable)	Detection and Fighting System	1	c

Table 4 – Telescope Structure expected minimum Safety Integrity Level

The remedial control measures to reduce risk to an acceptable level (based on the Preliminary Hazard Analysis and Risk Assessment) shall be discussed with CTAO to assess and agree the required SIL or PL level such safety system shall have.

2.5.7 Failures

None of the following cases shall lead to *catastrophic* or *critical* hazard severity (Section 2.3.1):

a) One or two independent operator errors,

b) One operator error plus one hardware failure,

c) One or two independent hardware failures,

d) One or two independent software failures.

e) Partial or complete loss of electrical energy supply

f) Lack of communication with the CTAO control system (ACADA)

Regarding these cases, it shall be noted that the analysis shall take into account that failures on certain SIL rated systems may be classified differently because of the possibility of very low likelihood of such failures.

2.5.8 Fault Conditions

The control system shall continuously monitor fault conditions that may affect the safety of equipment or personnel and shall automatically enter fault mode if a serious fault is detected. Serious faults include, but are not limited to:

a) Excessive motor current

b) Motor overheating

c) Large servo oscillation/ instability

d) Critical sensor fault (especially an encoder) or power failure

e) Overspeed of the azimuth or altitude axis

The overspeed monitoring system shall be independent of the main axes encoders. Any error condition that may cause overspeed shall not have the potential of also leading to a malfunction of the overspeed monitoring system.

2.5.9 Automatic parking conditions

The telescope structure shall automatically move to parking conditions when no command or time signal is received for a time settable to 1 minute to 60 minutes.

The hazard analysis shall identify if additional conditions (environmental or others) shall cause the structure to move to parking conditions automatically.

2.6 Fire Safety

2.6.1 General

The telescope shall limit to a minimum any fire loads to the extent technically possible.

This includes the choice, when reasonably possible[5], of fire-resistant cabling according to AD09.

2.6.2 Fire detection and fighting system

Fire detection shall be implemented in the telescope structure. The telescope shall be designed for compliance with fire regulations.

Firefighting measures shall be discussed and agreed with CTAO.

[5] High flexibility cables for use in cable wrap or similar may not comply with AD09.

2.7 Other Safety Features

2.7.1 Lockout / Tagout

RD03 and later amendments specify the minimum requirements concerning safety and health for the use of work equipment. Paragraph 2.14 of the EHSR specifies that *"All work equipment must be fitted with clearly identifiable means to isolate it from all its energy sources. Reconnection must be presumed to pose no risk to the workers concerned."*

The telescope structure shall be designed so that installation, maintenance, or repair operations can only be carried out when the work equipment is shut down. The work equipment and all its moving parts must be protected against accidental start and movement. To ensure this, appropriate lockout and/or tagout devices to energy isolating devices shall be provided to disable machines or equipment an unexpected energization, start up or release of stored energy. The systems or equipment involved shall be designed to enable these features (e.g. by means of a mains switch that is lockable in the 'off' position for the electrical supply, visible isolation).

A review shall be part of the risk analysis to determine which switches, valves, or other energy isolating devices apply to the equipment being locked out. More than one energy source (electrical, mechanical, hydraulic, pneumatic, chemical, thermal and gravitational) may be involved.

Lockout / tagout shall be physically implemented in an easily accessible place, and its location shall be agreed with CTAO. Lockout / tagout means shall be based on individual locks and not on interchangeable keys.

2.7.2 Local Disable

A selective local disable function of the structure axes shall be available for maintenance purposes. It shall be based on a switch that cuts the power to the drive and at the same time interlocks the corresponding subsystem causing the brakes to be engaged. The location of the local/remote selector shall be agreed by CTAO based on hazard considerations under aspects of visibility and access.

2.7.3 Local Control Panel

A local control panel shall be provided for local control and command of the structure rotation axes. The location of this panel shall be chosen under ergonomic and safety considerations, whereby the visual observation of the movement may be necessary. An emergency stop shall be included at the panel.

2.7.4 Portable Control Unit

A portable control unit shall be provided for use of maintenance personnel servicing the telescope structure. This shall provide at least velocity control loop in both Altitude and Azimuth axes, only when the control has been put in Local.

The portable control unit shall be equipped with an emergency stop, velocity control setting adjustment, and provide the encoder reading on a display.

2.8 Other Safety Provisions

2.8.1 Protection from Falling from Height

Provisions for access shall be given for maintenance activities. If permanent access means are installed, these should be approved by CTAO and fitted with appropriate safety provisions as per EN ISO 14122 [AD12] (guardrails, toe boards etc…).

Ladder access shall be allowable provided adequate means of fall arrest are pre-installed.

There shall be a thoroughly implemented system to prevent hazards from falling objects that may cause injuries to personnel.

The telescope structure shall by default prevent any altitude axis movement, as long as there is any human presence in or near the altitude structure. It should be evaluated if this can be implemented based on a physical interlock system rather than or in addition to a safe work procedure.

2.8.2 Protection From Falling Objects

To adequately address the risk of objects falling, there shall be a thoroughly implemented system to prevent hazards from falling objects to occur. This applies to damages to subsystems (especially the reflective mirrors) and pointing camera or similar devices. This may lead to:

- Screws shall be locked in position to avoid unscrewing.
- Procedures in maintenance manual to ensure that tools and equipment is not left in the altitude structure.
- Installation of toe boards.
- Others to be defined.

2.8.3 Laser Safety

The following provisions shall be considered when laser equipment is used:

- Laser equipment on machinery must be designed and manufactured to prevent any accidental radiation.
- Use of optical equipment for the observation or adjustment of laser equipment must not pose any risk to health.
- Laser equipment on machinery must be protected so that radiation, radiation produced by reflection or diffusion and secondary radiation do not damage health.

2.8.4 Access Security

In the cases where an external fence around the telescope is foreseen, there shall be protection against the access of unauthorized personnel by a lock on the gate to the telescope area. The need for implementing a sensor on the gate and/or a monitoring system shall be considered.

In the case where no individual fences around the telescope, there shall be protection against the access of unauthorized personnel to the telescope structure and cabinets (e.g. by locks on doors cabinets, sensors to monitor the tower door and/or similar provisions).

2.8.5 Hatches

Hatches which may inadvertently be left open shall be provided with sensors and/or interlocks.

Hatches which may be used for alternate access or egress shall be equipped with means for opening from outside.

2.8.6 Others

Other safety provisions not specifically mentioned in this document are listed in the Product Safety Plan [AD04].

2.9 Hazardous Material

2.9.1 Requirements

The use of any hazardous and/or flammable material shall be limited to a minimum, to the extent technically possible.

Hazardous material used shall be identified and declared in a HML (Hazardous Material List)

2.9.2 Materials

The telescope design shall comply with the European Directive 2011/65/EU (RoHS Directive) of the European Parliament and of the Council of 8 June 2011 and the amending Directive 2015/863/EU of 4 June 2015 [AD23], [AD24].

Materials (and materials used in surface treatments) identified in the Regulation (EC) No 1907/2006 [RD04] of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH), are not to be used by the telescope design.

All adhesives, coatings, and paints shall be non-hazardous in the cured condition.

3 Safety Documentation Package Preparation

The following safety documentation package shall be delivered to CTAO according to the Document Requirement Definition herein.

3.1 DRD Hazard Analysis

The Hazard Analysis, along with the hazard material list, shall be prepared in two steps. In a first step, the following work shall be performed:

- Establish the preliminary hazard list, and the risk assessment as part of the preliminary Hazard Analysis.
- Establish a hazardous materials list (chapter 3.2) related to the telescope structure, if relevant.
- Include in the design all the safety features and provisions according to the safety requirements included in this safety specification for telescopes and the result of the telescope structure safety analysis.
- Treat as relevant, the aspects of fire safety.

In a second stage, and after having discussed with CTAO the preliminary hazard analysis, the following activities shall be performed:

- Update the hazard analysis and ensure by implementing the appropriate risk reduction measures (e.g. safety control systems with the appropriate SIL, applied provisions from harmonized European standards) that all residual risks related to hazards identified have been brought into compliance with the hazard acceptability requirements of this safety specification for telescopes.

This flow down of activities assumes a two-step design process with a Preliminary Design Review and a Final Design Review. The activities can be combined in the case of a Critical Design Review allowing production to start, in case of a successful review outcome.

The hazard analysis report shall apply the general principles of EN ISO-12100:2010 (AD06) and finally contain as a minimum:

- Description of the Subsystem
- List of hazards, including the hazards depending on the adopted design and the operational hazards
- List of all the environmental and accidental hazards
- Evaluation of the Risk Priority Numbers including severity of the effect, likelihood of occurrence and ability of detection
- Explanation of the risk reduction measures adopted
- Any input to operation and maintenance procedures
- Demonstration of the acceptability of the residual risks
- Conclusions.

3.2 DRD Hazard Material List

The document shall contain the following information:

1. Hazardous Materials (HAZMAT) identification

2. HAZMAT Categorization

   a. Restricted HAZMAT
   b. Tracked HAZMAT

3. HAZMAT data tracking (restricted and tracked HAZMAT included in the delivered system, subsystems and support)

   a. HAZMAT item or substance name
   b. HAZMAT Category (restricted, or tracked)
   c. Location of HAZMAT within the system
   d. Quantity of HAZMAT within the system
   e. Application, process, or activity whereby quantities of HAZMAT are embedded in the system, or used during operations and maintenance
   f. Reasonably anticipated HAZMAT possibly generated during the system's life-cycle (e.g., installation, test and evaluation, normal use, and maintenance or repair of the system)
   g. Special HAZMAT control, training, handling measures and Personal Protective Equipment (PPE) needed.

3.3 DRD Safety Compliance Assessment Report

In accordance with the CTAO Product Safety Plan AD04], the telescope designer and/or subsystem designer shall prepare a safety compliance assessment report documenting the implemented mitigations and safety compliance activities according to the hazard analysis, the technical specification and to the applicable safety related standards.

The safety compliance assessment report shall demonstrate compliance with specified, national or industrial codes or this CTAO safety specification and regulations to ensure the safe design of the product and to comprehensively evaluate the safety risk being assumed prior to test or operation.

3.3.1 CDR level

At CDR level the safety compliance assessment report shall document the safe design of the telescope structure.

The safety compliance assessment report shall be ready in its final form at the Test Readiness Review milestone, and hence at provisional acceptance. In its final form it shall comprehensively document all the compliance activities, showing item per item all identified risks and all the measures of mitigation applied and the final residual safety risk prior to operation.

As such, in its final form the assessment shall include information from the hazard analysis prepared during the design phase and all other analyses, and reports of verification activities like inspections and test reports related to safety that are deemed necessary to comprehensively confirm the safe design, operation and maintenance of the system and its subsystems.

This includes (but is not limited to):

- A description of the system and/or subsystem(s) and their interfaces.

- The hazard analysis including the risk assessment.
- Information on all safety related design measures and safety functions including the report of the SIL/PL of the safety related control systems.
- Information on residual risks with identification of specialized procedures, skills, trainings, and Personal Protection Equipment (PPE).
- The identification of specialized safety requirements: the designer should identify all safety precautions necessary to safely operate and support the Product. This includes applicable precautions external to the Product or outside the designer responsibility such as off-the-shelf equipment, personal safety equipment, personnel safety skills and training, operational requirements involving CTAO, etc.
- The identification of hazardous materials and the precautions and procedures necessary for the safe handling of the material.
- Reference to all standards, requirements and other sources including version, date and issue number.

3.3.2 TRR level / Acceptance level

The documentation provided at CDR level shall be complemented at TRR and not later than at acceptance by CTAO with:

- The results of any audits / inspections carried out.
- The test reports of the safety verification performed on the hardware, or any other analyses and inspections related to safety, to demonstrate compliance with standards and with the present specification.

The safety compliance assessment shall also include a include a Declaration of Conformity (DoC) drafted in accordance to International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17050-1:2004 [AD22] and a Declaration of Incorporation (DoI) where applicable. The DOI, to be used for partly completed machinery, shall state that the subsystem/equipment must not be put into service until the machine into which it has been incorporated has been declared in conformity. The partly completed machinery must be supplied with information containing a description of the conditions which must be met with a view to correct incorporation in the final machinery, so as not to compromise safety.

3.3.3 As-Built Configuration

If needed the Safety Compliance Assessment Report shall be updated to record any impact of late (post-design, post-TRR) changes or the final as-built configuration.

3.4 DRD FTA

Fault tree analysis (FTA) is concerned with the identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event. With FTA this event is usually seizure or degradation of system perfomance, safety or other important operational attributes.

The FTA analysis shall contain the following information as a minimum:

- Description of the system under examination
- Assumptions used in the analysis
- Identification of the failure modes
- Analysis of the failure effects and causes
- Classification of the failure by severity
- Criticality calculations
- Rank failure mode criticality
- Determination of the critical items
- Identification of the means of failure detection, isolation and compensation
- Identification of special controls necessary to reduce failure risk
- Recommendations
- Follow up on corrective action implementation/effectiveness

The result shall highlight the failure causes with relatively high probability and severity of consequences, identifying the remedial effort and corrective actions required.