SST Mechanical Structure: Safety System

SST-MEC-DSR-002

Version 1a

Prepared by:		
Gino Tosti (INAF)		SST-STR SE
Salvatore Scuderi (INAF)		SST-STR PM
Alessio Trois (INAF)		SST-PRO PRM
Nicola La Palombara (INAF)		SST-PRO PRQM
Approved by:		
Gianpiero Tagliaferri		SST-ESC

Current Release				
Ver.	Created	Comment	Distribution	Editor(s)
1a	01/08/2023	First Issue	SST Consortium, CTAO	Gino Tosti

Version History				
Ver.	Created	Comment	Distribution	Editor(s)

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 Scope & Purpose

The scope of this document is to describe, after an SST Overview, the SST safety system, that is part of the Mount Local Control System, focusing on the interlocks chain and safety and unit logic, with the purpose to give a representation of the safety functionalities that SST has to guarantee to assure scientific and technical operations safely.

1.2 Applicable Documents

The following documents, of the exact issue shown, form part of this specification to the extent specified herein. In the event of a conflict between the documents referenced herein and the content of this document specification, the content of this document specification shall be considered as a superseding requirement.

[AD1] SST Programme: Telescope Technical Requirements Specification, SST-PRO-SPE-001
[AD2] CTA Software Programming Standards, CTA-STD-OSO-000000-0001, 23 January 2020
[AD3] CTA ACADA - Array Element Logging ICD, CTA-ICD-SEI-000000-0005, 2 June 2021

[AD4] CTA Array Element Monitoring, CTA-ICD-SEI-000000-0004-1b,
[AD5] SST Mechanical Structure: Mount Control System, SST-MEC-SPE-004
[AD6] CTAO System Control Concept, Doc. No: CTA-TRE-SEI-000000-0016-1a, 5 October 2022
[AD7] CTAO System Control Development Guidelines, CTA-TRE-SEI-000000-0017-1a-Draft 03, 15 January 2022
[AD8] Telescope Safety Design Specification, CTA-SPE-TEL-000000-0003_1a, 18 January 2023
[AD9] ICD Between IPS and Telescopes, Doc. No CTA-ICD-SEI-000000-0027- Draft 1c, 11 March 2022

1.3 Reference Documents

[RD1] SST Programme: Telescope Architecture and Design Summary Report, SST-PRO-DSR-002, version 1b, 08-Nov-2022
[RD2] Camera Design Report, SST-CAM-DSR-001, Version 2.a, 23-Nov-2022
[RD3] Mechanics Design Report, SST-MEC-DSR-001, Version 2.a, 30-Nov-2022
[RD4] Optics Design Report, SST-OPT-DSR-001, Version 1a, 25-Nov-2022

1.4 Definition of Terms and Abbreviations

ACADA	Array Control and Data Acquisition System

ACS	ALMA Common Software
AMCU	Active Mirror Control Unit
AIV	Assembly, Integration, Verification/Validation
ASTRI	Astrophysics with Italian Replicating Technology Mirrors
CDR	Critical Design Review
CTA	Cherenkov Telescope Array
CTAO	Cherenkov Telescope Array Observatory
ICD	Interface Control Document
GUI	Graphic User Interface
HW	Hardware
INAF	Istituto Nazionale di Astrofisica
IPS	Integrated Protection System
LCS	Local Control System
LPC	Low Power Cabinet
MACS	Mount Axes Monitoring Software
MCH	Mount Control Hardware
PDR	Preliminary Design Review
PLC	Programmable Logic Controller
PMC	Pointing Monitoring Camera
SDD	Software Design Document
SDLC	Software Development Life
STO	Safe Torque Off
SRS	Software Requirements Specification
SST	Small Sized Telescope
SST-CAM	SST Camera
SST-STR	SST Structure
STO	Safe Torque Off

SUM	Software User Manual
SVerP	Software Verification Plan
SValP	Software Validation Plan
SW	Software
TBD	To be determined
TBC	To be Confirmed
TCS	Telescope Control System
TBC	To be Confirmed
TCU	Telescope Control Unit
THCU	Telescope Health Control Unit
UC	Use Case
UCD	Use Case Document
WP	Work Package
WPD	Work Package Description
WBS	Work Breakdown Structure
PA	Product Assurance

1.4.1 Glossary

Table 1: Glossary of main terms used in the SST project.

TERM	DEFINITION
SST Programme	The overall SST organisational structure containing the SST-STR and SST Cam projects.
SST-STR	The SST Structure, consisting of elements under the control of the SST-STR Project.
SST-CAM	The SST Camera, consisting of elements under the control of the SST-CAM Project.
Central Facilities	Used as a catch-all in this document for on-site facilities not located at the Telescope Unit.
On-site Data Centre Farm	The central computing and storage facility on which all data is stored and all software installed.
Clock Distribution	The part of the central facility responsible for the provision and distribution of clocks for the precise time-tagging of images recorded by the Camera Unit.
Central Power Distribution	The part of the central facility responsible for distributing power to each Telescope Unit.
Central Site Safety System	The part of the central facility responsible for human safety, coordinating and acting upon safety information from all telescopes and other devices.
SST Software	All SW installed on the Farm that is under the responsibility of the SST Programme.
Telescope Manager	Part of the SST SW dealing with the high-level control interface to ACADA.
Camera Manager & DAQ	The SST SW dealing with the control of the Camera Unit and Camera Support Systems. Part of SST-CAM.
Structure Manager	The SST SW dealing with the control of the Structure. Part of the SST-STR.
Telescope Unit	All elements of a telescope located locally at that telescope.
Foundation	The physical foundation on which the Telescope Structure is mounted. Part of the Telescope Unit.
Interface Cabinet	The CTAO-controlled interface for power, network and timing connection to the telescope.
Telescope Structure	The telescope mechanical structure drives and optics.
Telescope Network Distribution System	The interface point from the Network Interface Cabinet to the telescope. Includes any patch panels, switches, associated mounting / housing and any fiber or copper cables routed about the Telescope Structure.
Telescope Control System	The control system for the telescope drives and any other active elements.
Telescope Safety System	Elements of the telescope explicitly for human safety, such as limit switches and access switches.
Telescope Power System	The interface point from the Power Interface Cabinet to the telescope. Includes any required hardware, associated mounting / housing and any cables routed about the Telescope Structure to other telescope elements.
Camera Unit	The physical camera as attached to the telescope structure.
Camera Support Systems	All support items required at the telescope to operate the Camera Unit, including the camera chiller, pipes.

2 SST Telescope Overview

When a VHE gamma-ray interacts with the atoms and ions in the upper levels of the atmosphere, it induces a cascade of secondary particles which propagate over many kilometres with a speed higher than the speed of light through the atmosphere. These particles emit Cherenkov light, forward-beamed with an opening angle of about one degree. A Cherenkov light event consists of a time-correlated multi-photon image with a typical timescale of ~10 ns. Cascades originate at an altitude of ~10 km above ground and create a light pool on the ground of ~120 m radius. Telescopes placed on the ground, containing large reflectors, focus the light to and imaging camera. Such Cherenkov cameras must be highly pixelated, cover a large field of view, and be able to detect UV/blue light down to the single photon levels with exposure times of approximately a billionth of a second. To provide a high imaging sensitivity over an extensive energy range, from a few tens of GeV up to a few hundreds of TeV, the Cherenkov Telescope Array Observatory (CTAO, see https://www.cta-observatory.org) will be made of sub-arrays with three different types of telescopes: large-sized (LST, 23 m diameter), medium-sized (MST, 12 m diameter) and small-sized (SST, 4 m diameter) telescopes. They are distributed in two observing sites, the Northern one in La Palma, the Canary Islands, and the Southern one in the Chilean Andes in the Paranal area. The CTA South "Alpha Configuration" would include LSTs, MSTs and SSTs. In particular, it envisages the construction and installation of 42 SSTs (a number that could increase up to 70 in future upgrades).

Table 2. Small-sized telescope main properties.

Small-Sized telescope (SST) main properties:	
Optical Design	modified Schwarzschild-Couder
Primary reflector diameter	4.3 m
Secondary reflector diameter	1.8 m
Effective mirror area (including shadowing)	>5 m2
Focal length	2.15 m
Total weight	17.5 t
Field of view	> 8.8 deg
Number of pixels in the SST Camera	2048
Pixel size (imaging)	0.16 deg
Photodetector type	SiPM
Telescope data rates (before array trigger)	>600 Hz
Telescope data rates (readout of all pixels; before array trigger)	2.6 Gb/s

Positioning time to any point in the sky (>30° elevation)	90s
Pointing Precision	< 7 arcsecs

More details about the SST Telescope design are described in [RD1], [RD2], [RD3], [RD4].

3 SST Control and Safety HW

The SST Safety System is considered part of the Mount Local Control System (MLCS), sketched in Figure 1.

The MLCS assembly includes all the electronics and hardware parts needed to drive the telescope safely to any accessible sky position during the commissioning, testing, maintenance and observing phases.

All HW devices for the control and management of the Mount and Safety shall be PC-PLCs and Safety PLCs (using Safety over Ethercat (FSoE)) - based on Beckhoff technology using the TwinCAT 3 environment as development and running platform (see Sections 5 and 6 for details).
The main MLCS control units are:

- The Telescope Control Unit (TCU), which is in charge of the monitoring and control of the major servo systems, internal power management for the health of all the subsystems on board the telescope (e.g., Cherenkov Camera, Pointing Monitoring Camera (PMC)).
- The Safety PLC which is in charge of the interlock chain management.

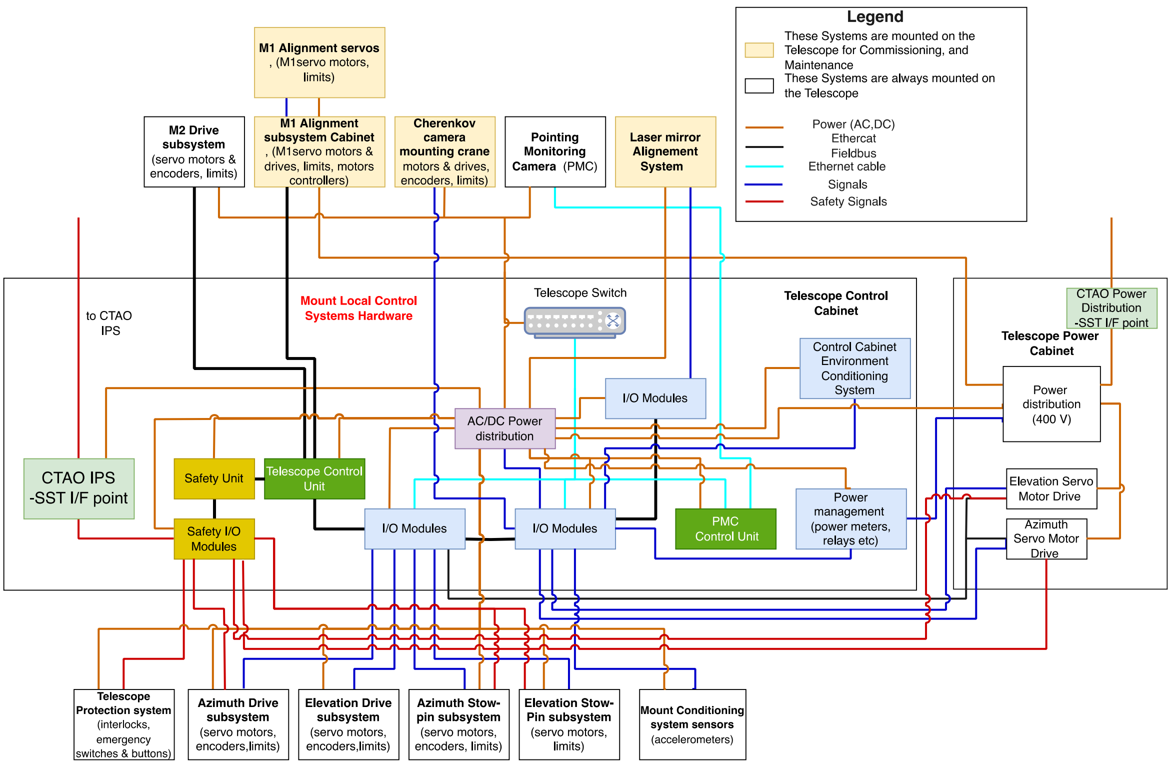


Figure 1. Mount Control HW Architecture and Connection Path.

3.1 Interlocks chain

The HW components related to the security system of the telescope can be grouped into three main sets of interlocks:

- Main Drive limit switches
- Stow Pin switches
- Emergency buttons and doors opening

All the interlocks devices that will be used in the SST Telescope shall be certified following the safety standards and they are of normally closed-circuit type (1 = not engaged, 0 = engaged).

3.1.1 Main drive Limit Switches

The main Drive limit switches are classified as software and hardware switch. SW switches are indicated as "AZ_Sw_CCW", "AZ_Sw_CW", "EL_Sw_LOW", "EL_Sw_HIGH".

The hardware switches ("AZOpCW", "AZOpCCW""AZEmCW", "AZEmCCW", "ELOpLOW", "ELOpHIGH", "ELEmLOW", "ELEmHIGH") are directional devices for which the physical trigger corresponds to a specific action dedicated to the protection of the physical limit of the motion, either for the Azimuth and Elevation axes. Each motion direction of both axes is equipped with two switches (Operational and Emergency) located at the physical limit of the axes motion range and dedicated to the stop of the axis in the current direction of the motion.

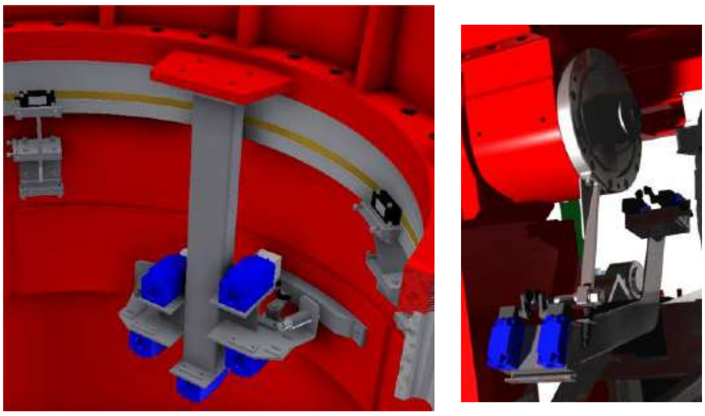


Figure 2. Azimuth (left) and Elevation (right) Main Drive Limit Switches.

3.1.1.1 Operational Limit Switches

The Operational limit switches engagement shall be Safety switch with a SIL = 2. They shall stop of the motion performed through a controlled ramp of deceleration retaining the possibility to move the axis only in the opposite direction. Safe Stop 1 (SS1) function will stop the motor drive in accordance with

IEC 60204-1. The Operational switches do not allow the drive to continue motion to angle wider than about 271° in both directions for Azimuth and +91° and -1° degrees in Elevation.

3.1.1.2 Emergency Limit Switches

The emergency limit switch shall be Safety switch with a SIL = 2. Their Engagement provides the immediate stop of the motion delivering no more power to the drive thorough the Safe Torque Off (STO) function. The STO function is a mechanism that prevents the motor drive from restarting unexpectedly, in accordance with IEC 60204-1, to preserve hardware from damages (see Section 0). Without these cautions the Azimuth cable wrap could suffer damages for excessive twisting.

The Emergency limits are located at an Azimuth angle of ±272° and Elevation angles of +92° and <-1°.

The complete list of the SST Main Drive switches with their positions and brief description are listed in the tables below.

Table 3. AZ Main Drive Limit Switches.

ID	Type	Description	Position
AZ_LYRE	Lyre	Information about the motion direction (clockwise or counterclockwise)	0°
AZ_OP_CW	Operational	Information about AZ motion limits in clockwise direction.	271.1°
AZ_EM_CW	Emergency	Information about AZ motion limits in clockwise direction	272.5°
AZ_OP_CCW	Operational	Information about AZ motion limits in counterclockwise direction	-271.1°
AZ_EMCCW	Emergency	Information about AZ motion limits in counterclockwise direction	272.5°

Table 4. EL Main Drive Limit Switches.

ID	Type	Description	Position
EL_OP_LOW	Operational	Information about EL motion limits in Horizon direction	-0.6° (*3)
EL_EM_LOW	Emergency	Information about EL motion limits in Horizon direction	-1.3° (*4)
EL_OP_HIGH	Operational	Information about EL motion limits in Zenith direction.	91.2°
EL_EM_HIGH	Emergency	Information about EL motion limits in Zenith direction.	92.2°

Notes:

- *the Lyre shall be inserted in the interlocks chain and managed directly by the Safety PLC.*
- *the safety system shall implement the SS1 function. When the Operational limit switches are engaged.*
- The Elevation *Emergency switch shall be located before the Elevation bumpers.*

3.1.2 Stow Pin Switches

The SST mechanical structure is provided with a stow pin systems, at least three insertion positions shall be present on the azimuth axis and one for the elevation to protect the telescope mirror from sun light and to ensure no motion when the telescope is in safe position (or parking), when maintenance operations are needed. The pin insertion into the specific witness is possible only when the telescope is at -90° position in Azimuth (Engineering frame [AD5]) and at the angle of 0° (parking position at South point).

The stow pin system related to each axis shall be equipped with switches providing some basic information on the pin status (fully extracted or inserted from witness) and when the axis is in correct position for the Pin insertion (Enabling). As a reference **Error! Reference source not found.** and Table 6 list the stow pin switches for the Azimuth and Elevation axes installed in the ASTRI prototype.

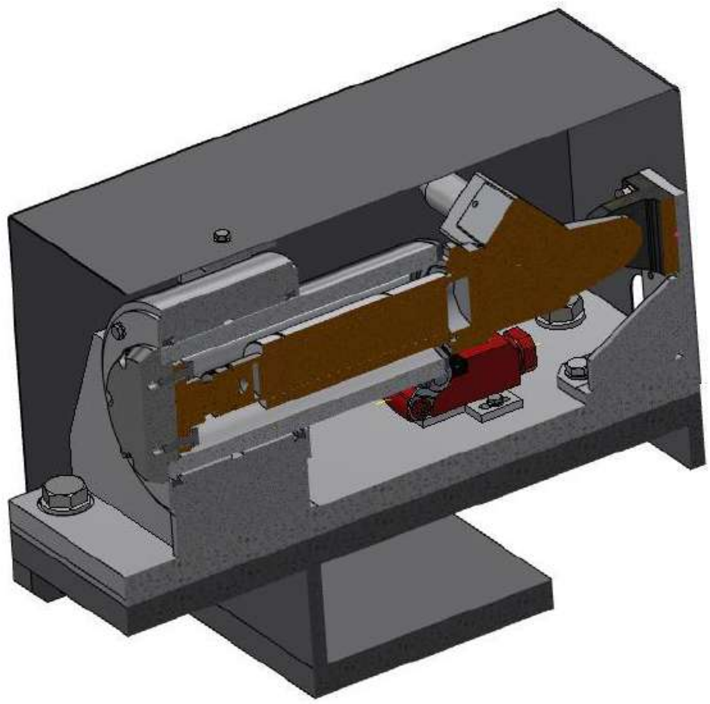


Figure 3. Section view of Azimuth stow pin.

Table 5. AZ Stow Pin switches.

ID	Type (Array)	Description	Position
AZSTOEN	Enabling	Notify the alignment between the pin shaft and the pin hole.	-90° (*[5])
AZSTOIN	Status	Notify the status of the AZ Pin insertion in the hole	-
AZSTOEX	Status	Notify the status of the AZ Pin extraction in the hole	-

Table 6. EL Stow Pin Switches.

ID	Type (Array)	Functionality	Position
ELSTOEN	Enabling	Notify the alignment between the pin shaft and the pin hole.	0° (Park) (*[5])
ELSTOIN	Status	Notify the status of the EL Pin insertion in the hole	-
ELSTOEX	Status	Notify the status of the EL Pin extraction in the hole	-

Notes:

- (*[5]) ***It is worth to note that the engagement range of Stow switch could be is too wide with respect the perfect alignment position between the shaft and the pin hole. Thus, the encoder position of the axes shall be taken into account to check the correct alignment in the parking procedure.***
- ***The positional switches should be not part of the Safety Logic Chain. They will be set as input in the hardware configuration of the telescope supervisor.***

3.1.3 Emergency Stop buttons and Doors switches

The SST Telescope shall be equipped with three emergency stops and switches providing the Cabinets and Base doors status (see Table 7). The emergency stops and the doors switches are inserted in the interlocks chain, as required by the safety standards, in order to stop immediately the motion of the Telescope through the (STO) function, when necessary.

The EMERG1 mushroom shall be located at the door of the Telescope Control Cabinet at eye level, while the EMERG2 is the emergency stop available on the hand-paddle used to move manually the telescope.

Table 7. Emergency mushrooms and doors opening switches.

ID	Type (Array)	Functionality	Position
EMERG1	Emergency Stop	When triggered the STO function is activated for both axes and the motion is inhibited.	Cabinet Door
EMERG2	Emergency Stop	When triggered the STO function is activated for both axes and the motion is inhibited.	Handle Paddle
DOORBASE	Door Opening	When triggered the STO function is activated for both axes and the motion is inhibited.	Door Base
DOORCAB	Door Opening	When triggered the STO function is activated for both axes and the motion is inhibited.	Doors Cabinets

3.1.4 Proximity/Prelimits Switches

The safety design of SST includes some additional switches called proximity/or Prelimits, which are not part of the interlock chain, but are used for the implementation of the SW procedures described in Section 6. The scope of those switches is to provide the Mount Control software with a physical trigger that the axes are in proximity of some motion limits (see Section 6.3) or that the telescope is close to one of the AZ/EL stow pin insertion position (during the parking/homing procedures, Section 6). The prelimits have the function to command a controlled deceleration of the motion.

As a reference Table 8 lists the prelimits installed on ASTRI-Horn. In ASTRI-Horn , as is required for the SST telescope too, each axis is equipped with three proximity switches: two are located few degrees before the Operational limits in both axes' directions, and one is positioned near the Stow Pins alignment switch.

Table 8. Emergency mushrooms and Doors opening switches.

ID	Type (Array)	Functionality	Position
AZSTOPRE	Proximity	When triggered the AZ axis slow down to 0.5°/s in order to reach the correct position for Pin insertion	-76.0°
AZLCW0	Proximity	When triggered in CW direction the AZ axis slow down to 0.5°/s	+261.0 °
AZLCCW0	Proximity	When triggered in CCW direction the AZ axis slow down to 0.5°/s	-261.0°
ELSTOPRE	Proximity	When triggered the EL axis slow down to 0.1°/s in order to reach the correct position for Pin insertion	4° (Horizon)

ELPLOW	Proximity	When triggered in Horizon direction the EL axis slow down to 0.1°/s	3.7°
ELPHIGH	Proximity	When triggered in Horizon direction the EL axis slow down to 0.1°/s	87.1°

This configuration shall be adapted to SST in which shall have more than one AZ stow pin insertion positions.

4 Safety Unit and Logic

4.1 Safety-PLC Architecture

The safety PLC architecture is described in Figure 4.

As already mentioned, the Safety PLC is functionally part of the TCU and shall use a Beckhoff Safety PLC (EL6910 or equivalent), and a number of I/O Safety modules (EL190X, EL290X) The physical architecture provides for switches and Emergency push-button to be connected to the Beckhoff input safe modules through a 24 V wiring system.

The output terminals shall be directly linked to the servo driver's safety clamps in order to activate the required safety Safe Torque Off (STO) function or SS1 based on the actual status of motion of the axes.

One or more inputs of the Safety-PLC shall be connected to the CTAO IPS system [AD9].

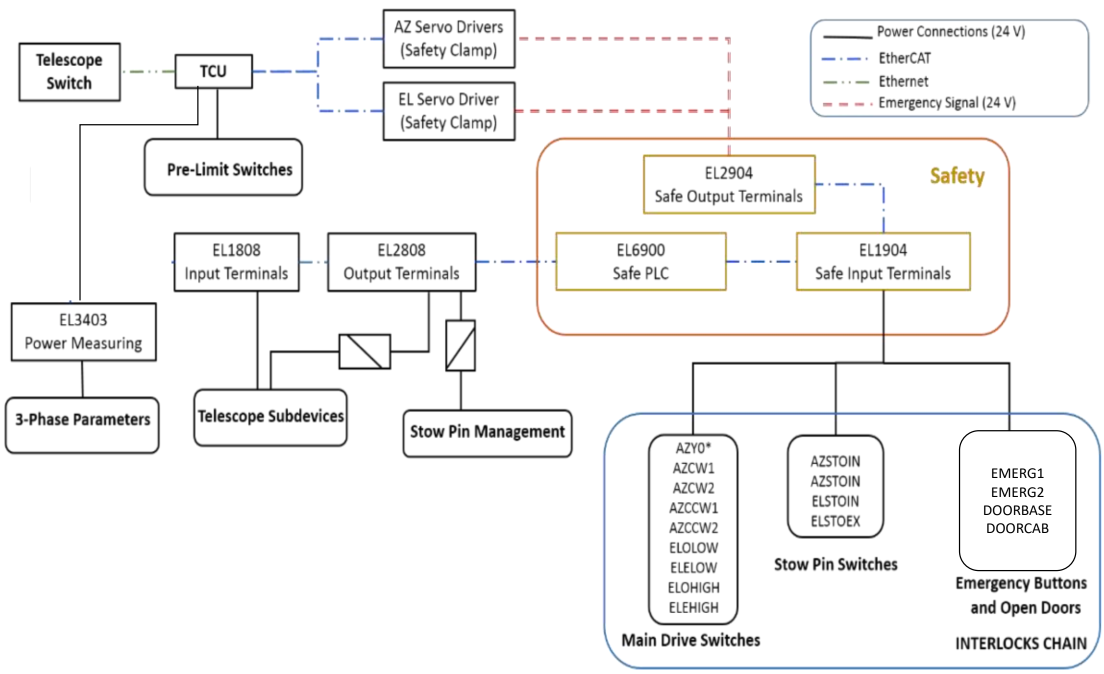


Figure 4. As Reference, this figure shows the Safety PLC HW including connection with telescope sub devices and interlocks chain as implemented in the ASTRI – Horn Telescope.

The Safety over Ethernet (FSoE) shall be the protocol used for the internal communication between the safety devices of the Mount control system. This solution was successfully used for almost 10 years in the ASTRI-Horn and is also used in the ASTRI Mini-Array. It offers high reliability, compactness, and low maintenance for the electronics of control, ensuring high real-time performances and a simplified environment for the development of safety applications.

4.2 Safety PLC Electrical Interface

The Input/Output safety modules needed shall be derived on the basis of the final design of the SST Telescope Safety system. These modules shall accommodate connection at least with:

- The Lyre device
- All the operational and emergency switches
- The Stow Pin engagement position switches
- Doors switches
- Dedicated input for the connection with the IPS system.

5 SST Interlocks chain Functional Description

This Section describes the safety functions associated to the triggers of the interlocks chain devices.

5.1 Safety Functions

5.1.1 Safety Torque Off (STO)

The STO function is the most common and basic drive-integrated safety function. It ensures that no torque-generating energy can continue to act upon a motor and prevents unintentional starting.

This function is a mechanism that prevents the drive from restarting unexpectedly, in accordance with EN 60204-1 As shown in Figure 5, after a physical trigger the Safe Torque Off function safely clears the pulses of the drive. The drive is reliably torque-free. This state is monitored internally in the drive.

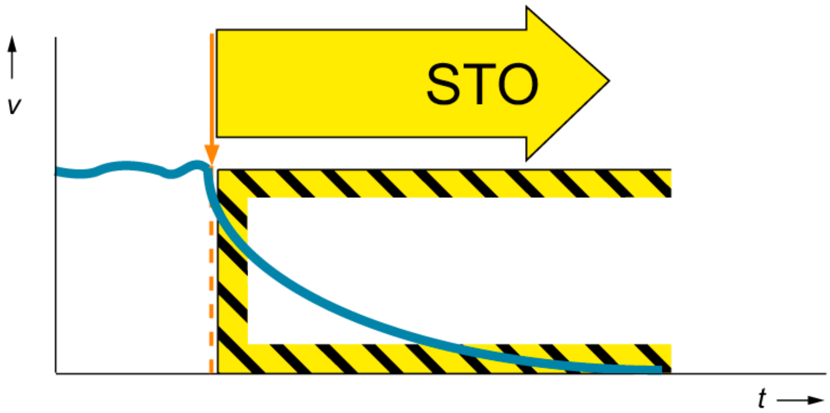


Figure 5. Safe Torque Off Function.

STO has the immediate effect that the drive cannot supply any torque-generating energy. STO can be used wherever the drive will be brought to a standstill in a sufficiently short time by the load torque or friction or where coasting down of the drive is not relevant to safety.

5.1.2 Safe Stop 1 (SS1)

The Safe Stop 1 (SS1) function causes a motor to stop rapidly and safely and switches the motor to exert no torque at all after coming to a standstill, i.e., STO is activated.

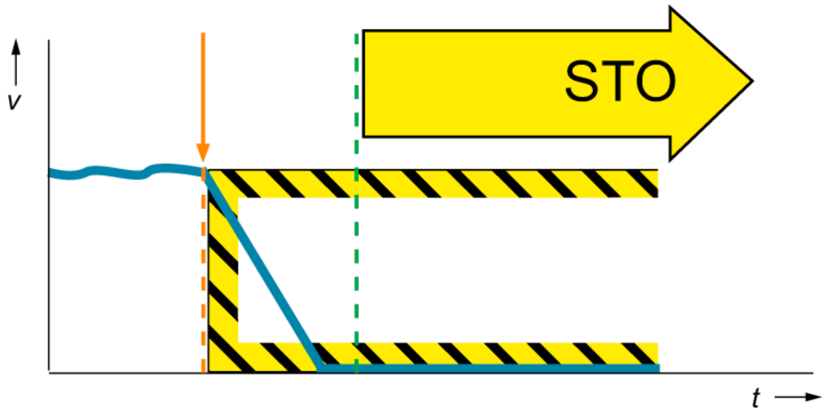


Figure 6. Safe Stop 1 function.

The Safe Stop 1 function can safely stop the drive-in accordance with EN 60204-1, Stop Category 1. When the SS1 function is selected, the drive brakes along a quick stop ramp autonomously and automatically activates the Safe Torque Off when the configured safety delay timer expires (See Figure 6).

The SS1 function is used to bring, in the event of a safety trigger, heavy masses in motion to a stop as quickly as possible and then enter the STO state.

5.2 Main Drive Limit Switches

Here we report, as reference, the list of actions activated when the safety switches are engaged. We will refer to the ASTRI-Horn system mainly, but the same function is also implemented in the ASTRI Mini-Array.

5.2.1 Action in case of Emergency Limits engagement.

The Emergency switch is triggered by the mechanical system and the related signal to the Safety PLC is delivered to the safe input module (EL190X).

- The Safety PLC (EL6910) activates the STO function and the 24V signals to both drives is cut off through the module EL290X (see Figure 1 red dotted line).
- Both axes are immediately stopped, and the motion is inhibited until the switch is disengaged and the STO status is not active. This can be done driving the system out of the switch with a Software acknowledge of the Alarms and a Reset of all errors. These two operations act as a sort of override (see Section 6) that will allow to move disengage the switch moving in the opposite direction.

5.2.2 Action in case of Operational Limits engagement.

The Operational switch is triggered by the mechanical system and the related signal to the Safety PLC is no more delivered to the safe input module (EL190X).

- The Safety PLC (EL6910) activates the SS1 function and the power to both drives is cut off through the Safety signal of EL2904 module, with a temporal delay after the trigger.
- The temporal delay allows the axis to pass over the triggered device and disengage it before stopping, while avoiding the engagement of emergency switch.
- The temporal delay must be calibrated considering the speed of motion and the deceleration ramp. (The motion speed after the pre-limit engagement is always 0.5 °/s for Azimuth and 0.1°/s for elevation).
- The axis is stopped in a position between the operational and emergency limit switch location while no one of them is engaged. In this situation the power to the drive can be switched on but the motion is permitted only in the opposite direction with respect the emergency limit switch position.

The tables below describe the functionalities and safety actions associated to the physical state of the Main Drive Limit Switches.

Table 9. AZ Main Drive limit switches functionalities.

ID	Status	Description	Safety Action
AZY0	0	The AZ axis is moving from 0 ° -270°	Enables counterclockwise limit switches and disables CW limit switches
	1	The AZ axis is moving from 1° +270°	Enables clockwise limit switches and disables counterclockwise limit switches
AZLCW1	0	The clockwise operational is engaged	SS1 function is active in clockwise direction. The AZ motion is allowed only in counterclockwise direction
AZLCW2	0	The clockwise emergency is engaged	STO function is active. The AZ motion is inhibited in any direction
AZLCCW1	0	The counterclockwise operational is engaged	SS1 function is active in counterclockwise direction. The AZ motion is allowed only in clockwise direction
AZLCCW2	0	The counterclockwise emergency is engaged	STO function is active. The AZ motion is inhibited in any direction

Table 10. EL Main Drive limit switches functionalities.

ID	Status	Description	Safety Action
ELOLOW	0	The Elevation low operational is engaged	SS1 function is active. The motion is allowed only in increasing elevation direction.
ELELOW	0	The Elevation low emergency is engaged	STO function is active. The EL motion is inhibited in any direction

ELOHIGH	0	The Elevation high operational is engaged	SS1 function is active. The EL motion is allowed only in decreasing elevation direction.
ELEHIGH	0	The Elevation high emergency is engaged	STO function is active. The EL motion is inhibited in any direction

5.3 Stow Pin Switches

When the AZ (EL) axis has reached the position (verified with main encoder axis) in which it is aligned with the stow-pin shaft and the stow-pin entrance hole, the switch AZSTOEN (ELSTOEN) is engaged (see Table 9):

- The voltage to the AZ (EL) motors is switched off and the drives are disabled. The pin is completely extracted and the related switch AZSTOEX (ELSTOEX) is engaged. Only in this case the stow Pin is allowed to be moved.
- The TCU commands the insertion of the pin and the AZSTOEX (ELSTOEX) switch is disengaged.
- The signals to the Safety PLC are no more delivered in the safe input module (EL190X) and the Safety PLC (EL6910) activates the STO function for both the axes. As soon as the stow-pin reached its motion limit the AZSTOIN switch is engaged, and the Pin stops to move. The STO function stops to act only when the Pin is completely extracted, and the axis can be moved again (see Section 6).

Table 11. AZ and EL Stow Pin Switches functionalities.

SWITCH	STATUS	DESCRIPTION	SAFETY ACTION	THCU ACTION
AZSTOEN	0	The AZ axis has reached the perfect alignment between the pin shaft and the pin hole.	No Action	AZ Pin can be inserted/extracted
AZSTOEN	1	The AZ axis is not aligned for the pin insertion	No Action	AZ Pin insertion is not permitted.

SWITCH	STATUS	DESCRIPTION	SAFETY ACTION	THCU ACTION
ELSTOEN	0	The EL axis has reached the perfect alignment between the pin shaft and the pin hole.	No Action	EL Pin can be inserted/extracted
ELSTOEN	1	The EL axis is not aligned for the pin insertion.	No Action	EL Pin insertion is not permitted.

SWITCH	STATUS	DESCRIPTION	SAFETY ACTION
AZSTOIN	1	The AZ stow pin is completely extracted.	No Action

AZSTOEX	0		
AZSTOIN	1	The AZ stow pin is extracting/ inserting	STO function for AZ Drive is Active
AZSTOEX	1		
AZSTOIN	0	The AZ stow pin is completely inserted.	STO function for AZ Drive is active
AZSTOEX	1		
AZSTOIN	0	The Status of the switches is undefined. A Fault is notified	STO function for AZ drive is active
AZSTOEX	0		

SWITCH	STATUS	DESCRIPTION	SAFETY ACTION
ELSTOIN	1	The EL stow pin is completely extracted.	No Action
ELSTOEX	0		
ELSTOIN	1	The EL stow pin is extracting/ inserting	STO function for EL Drive is Active
ELSTOEX	1		
ELSTOIN	0	The EL stow pin is completely inserted.	STO function for EL Drive is active
ELSTOEX	1		
ELSTOIN	0	The Status of the switches is undefined. A Fault is notified	STO function for EL drive is active
ELSTOEX	0		

5.4 Emergency and Open doors

The functionalities of the devices belonging to this category has been already described in Table 7. For the details of the logic chain developed see Section 6.

6 SST Safety Logic Software

The software of control for the Mount system of the SST telescope Shall be developed using the TwinCAT 3 (TC3) environment platform provided by Beckhoff. The TC3 makes available a dedicated module for the safety applications (TwinSAFE), through which the logic management of the interlock's signals shall be implemented.

6.1 Implementation

The physical signals of devices connected to the safety chain is mapped into the TC3 system as variables in order to develop the Safety functionalities STO and SS1 described in 5.1: each busy channel of the Safety Input modules (EL190X) is associated to a Boolean variable whose status reproduces the electrical signal provided by the physical device. If the physical switch is not engaged the electrical circuit is closed and the status of the associated variable is TRUE, on the contrary if the device is engaged the circuit is opened and the variable value is FALSE.
The states of Boolean variables can be managed by making use of specific safety (standard-certified) Function Blocks (see **Error! Reference source not found.** as example), to implement logic of the output signal for the safety clamps of the servo drives of the motors.
The output module (EL290X) of the safety hardware delivers one signal to each safety clamps of the AZ and EL servo drives. This module is able to deliver or not deliver a 24 Volt signal to each servo drive safety input, based on the Safety logic. For example, if one of the limit switches is engaged, or one of the telescope doors is opened (Cabinet or Base) or an emergency button is pushed, the Safety module immediately stops the delivery of the 24 Volt signal to the drives inhibiting their operation (as described in?). This means that, if the telescope was moving the motors are safely stopped and the motion is inhibited until the STO signal is repristinated.

As soon as the emergency situation is recovered by the user (no automatic exit strategy from an emergency situation shall be implemented) the Safety PLC restores the 24 V delivery to the servo drives and the telescope can restart operations. For security reasons whenever a STO/SS1 function is activated the Mount Control Software running on the TCU is able to switch off the high voltage to the motors and to disable the servo drives.

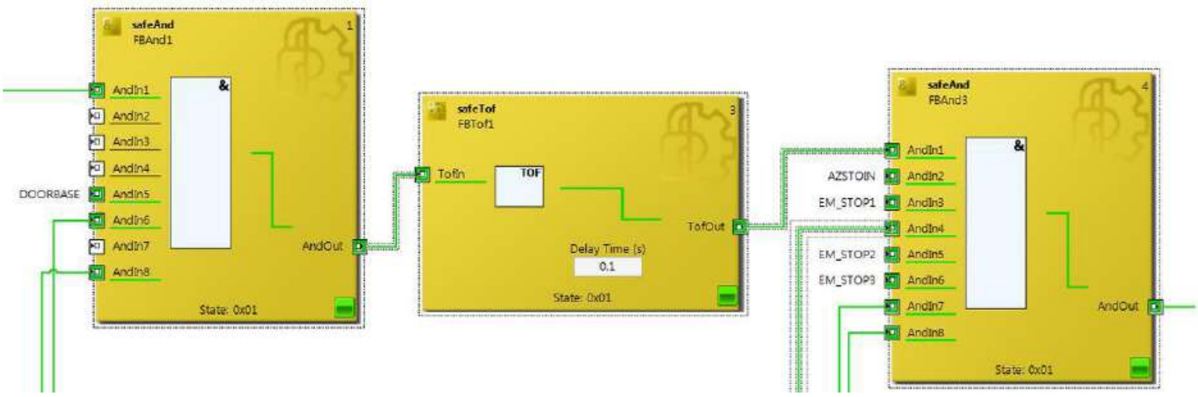


Figure 7. Example of the interlock logic chain implementation managed by the Safety PLC performing the STO function. Each logic module can have one or more inputs which status corresponds to the physical signal of the interlocks (e.g. the Switch for the base of the door (DOORBASE)) and returns in output the suitable logical combination of these signals, based on the logical operator selected (e.g. SafeOR, SafeAND).

6.2 Logic Chain

In this section are presented the Logic Gate flows of the signals related to the devices of the interlocks chain.

In Figure 8 is described the logic gate flow of the AZ Main Drive Limit switches. The STO functions are developed for the emergency limits switches while the SS1 functions are implemented for the Operational devices in both direction (CW and CCW).

The Figure 9 reproduce the logical operation needed for the implementation of the SS1 and STO functions of the Elevation Main drive limit switches. The STO functions related to the Emergency push-button and doors status switches are sketched in Figure 10.

It has to be noted that the final logical signals provided by AZ and EL Main drive switches block are inserted in the final SafeAND of each other. This is because even if the trigger signal comes only from one axis it shall be required that both axes will be safely stopped.

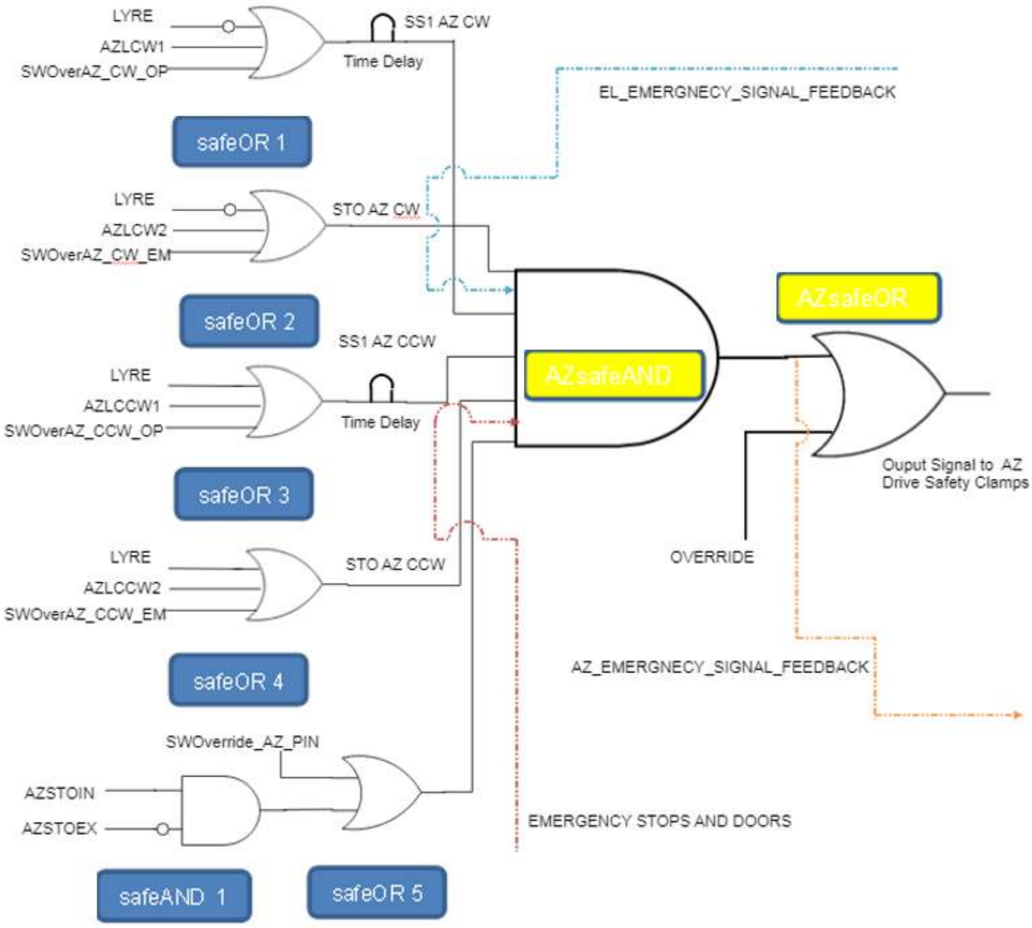


Figure 8. Logic gate flow of the AZ Main Drive Limit switches.

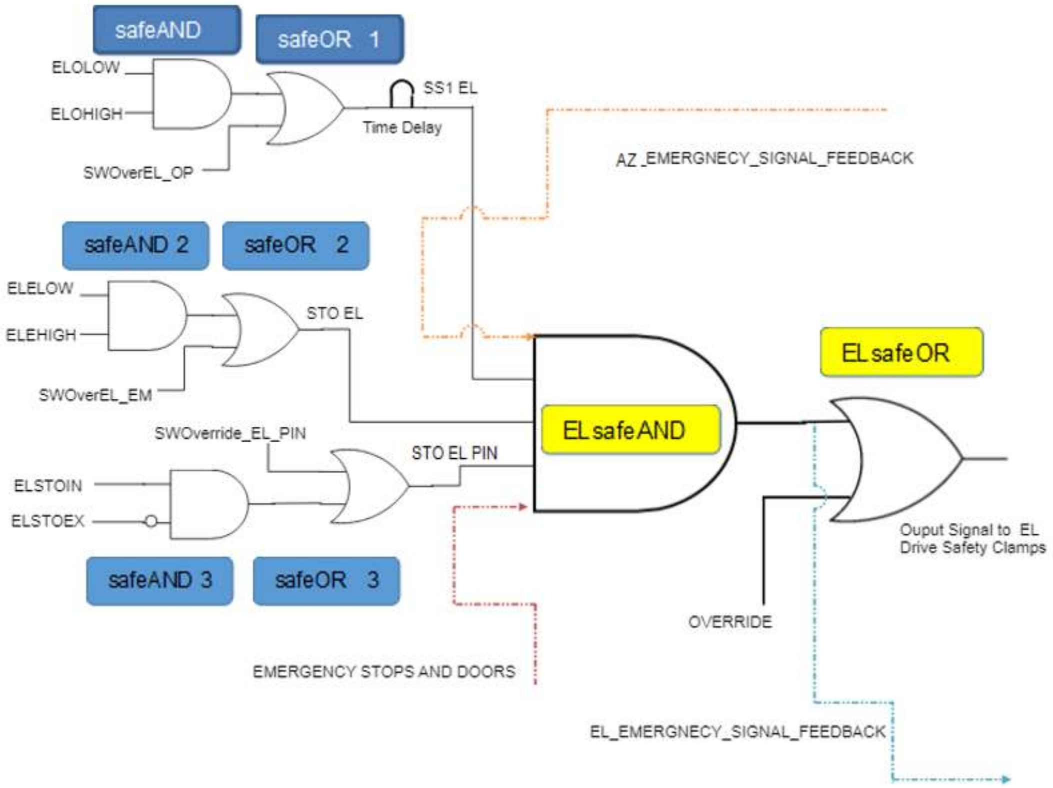


Figure 9. Logic gate flow of the EL Main Drive Limit switches.

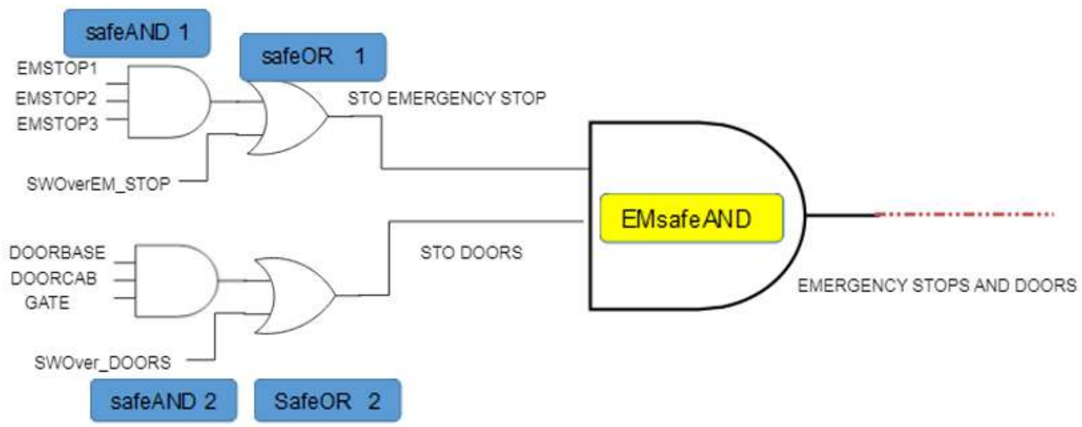


Figure 10. Logic gate flow of the Emergency stops and Doors status switches.

The combination tables of the logic chain implementation are available in the following tables.

Table 12. AZ Main Drive limit Switches Logic Gate.

SafeOR 1			To AZSafeAND
Not LYRE	AZLCW1	SWOver_CW_OP	GATE
0 (1)	1	0	1
0 (1)	0	0	1
1(0)	0	0	0 (SS1)

SafeOR 2			To AZSafeAND
Not LYRE	AZLCW2	SWOver_CW_EM	GATE
0 (1)	1	0	1
0 (1)	0	0	1
1(0)	0	0	0 (STO)

SafeOR 3			To AZSafeAND
LYRE	AZLCCW1	SWOver_CW_OP	GATE
1	1	0	1
1	0	0	1
0	0	0	0 (SS1)

SafeOR 4			To AZSafeAND
LYRE	AZLCCW2	SWOver_CW_EM	GATE
1	1	0	1
1	0	0	1
0	0	0	0 (STO)

Table 13. AZ Stow Pin Switches Logical Table.

SafeAND 1		SafeOR 5		To AZSafeAND
AZSTOEX	AZSTOIN	GATE	SWOver_AZ_PIN	GATE
0	1	1	0	1 (Extracted)
1	1	0	0	0 (STO, Inserting/extracting)
1	0	0	0	0 (STO, Inserted)
0	0	0	0	0 (STO, Anomaly)

Table 14. EL Main Drive Limit Switches Logical Table.

SafeAND 1		SafeOR 1		To ELSafeAND
ELOLOW	ELOHIGH	GATE	SWOver_EL_OP	GATE
1	1	1	0	1
0	1	0	0	0 (SS1)
1	0	0	0	0 (SS1)
0	0	0	0	0 (SS1)

SafeAND 2		SafeOR 2		To ELSafeAND
ELELOW	ELEHIGH	GATE	SWOver_EL_EM	GATE
1	1	1	0	1
0	1	0	0	0 (STO)
1	0	0	0	0 (STO)
0	0	0	0	0 (STO)

Table 15. EL Stow Pin Switches Logical Table.

SafeAND 3		SafeOR 3		To ELSafeAND
ELSTOEX	ELSTOIN	GATE	SWOver_EL_PIN	GATE
0	1	1	0	1 (Extracted)
1	1	0	0	0 (STO, Inserting/extracting)
1	0	0	0	0 (STO, Inserted)
0	0	0	0	0 (STO, Anomaly)

Table 16. Emergency Stops Logical Table.

SafeAND 1			SafeOR 1		To EMSafeAND
EMERG1	EMERG2		GATE	SWOver_EM_STOP	GATE
1	1		1	0	1
0	1		0	0	0 (STO)
1	0		0	0	0 (STO)
1	1		0	0	0 (STO)

Table 17. Open Doors Logical Table.

SafeAND 2			SafeOR 2		To EMSafeAND
DOORCAB	DOORBASE	GATE	GATE	SWOver_Doors	GATE

1	1	1	1	0	1
0	1	1	0	0	0 (STO)
1	0	1	0	0	0 (STO)
1	1	0	0	0	0 (STO)

Table 18. EL blocks final combination.

ELSafeAND		ELSafeOR		El drive
SS1 EL	STO EL - STO EL PIN - AZ_FEED - EM & DOORS	GATE	OVERR	GATE
1	1	1	0	1
0	1	0	0	0 (SS1)
1	0	0	0	0 (STO)
0	0	0	0	0 (STO)

Table 19. AZ blocks final combination.

AZSafeAND		AZSafeOR		AZ drive
SS1 AZ CW-CCW	STO AZ (CW,CCW) - STO AZ PIN - AZ_FEED - EM & DOORS	GATE	OVERR	GATE
1	1	1	0	1
0	1	0	0	0 (SS1)
1	0	0	0	0 (STO)
0	0	0	0	0 (STO)

6.3 Pre-Limit Software Safety

Despite the physical limits of the motion are protected by the appropriate safety devices and logic, the safety system of the SST telescopes provide also for the proximity devices described in Section 5. Those devices are connected to the hardware configuration of the (TCU) and are used to develop some additional security measures carried out by specific functions implemented in the Mount Control

Local Software and available for each axis during normal operations: Slow Down and Software Safety Stop (optional).

The Slow Down is in charge of the constant monitoring of the axis position and velocity during the motion and to command a slow down to a constant velocity of the axis (0.5°/s for AZ and 0.1°/s for EL) whenever the proximity switch, related to that direction is engaged, rising a warning. If the motion won't be stopped by the user, the Software Stop will come into action and automatically stop the axis before the Operational limit switch is engaged, allowing the motion only possible in the opposite direction of the Limit switches.

It has to be noted that the Slow Down function is also important for the correct implementation of the SS1 function. In particular make it easy the calibration of the time delay to apply keeping always constant the speed at which the axes will eventually reach the Operational Limits.

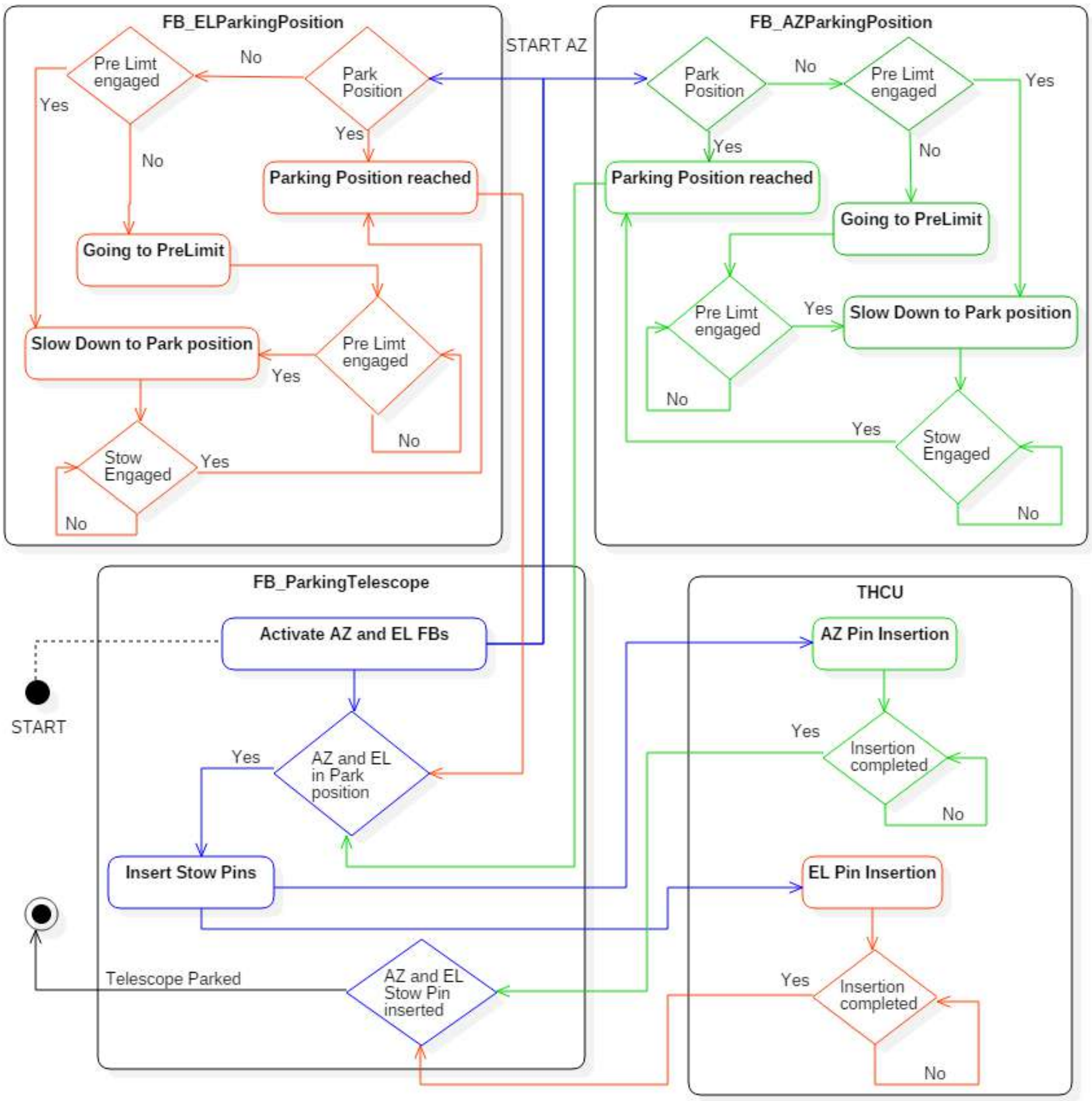
6.4 Parking Procedure

The Parking procedure moves the telescope to a safe position, to avoid sunlight focusing, during the day. In the South hemisphere the parking position provide for the Elevation axis point to the horizon (EL=0°) and the Azimuth axis faces at North (AZ=90° in ENG coordinate system). Furthermore, in order to prevent damages to the mechanical structure (may be caused by strong gusts of wind or minor earthquakes), when the telescope reaches the parking position the Azimuth and Elevation Stow Pins are automatically inserted. The Parking procedure is managed by the Mount Local Control Software running on the TCU.

When the procedure is triggered by a change of telescope state by the user or triggered by a prolonged state of inactivity of the telescope. The axes of the telescope move toward the safe position with a constant velocity of 1.5°/s along the Elevation axis and 2°/s along the Azimuth. As soon as the Proximity limit switches for the Stow Position are reached (see Section 5), the AZ axis slow down to 0.5 °/s, while EL to 0.1°/s. The axes will stop when the Stow limit switches are engaged, and a specific position value is read by the encoders of each axis. Only when both axes are stopped, meaning that the parking position has been reached, MCS Local control Software command the Stow Pins insertion.

The flow diagram for the Parking procedure implementation is shown in Figure 11.

Figure 11. Slow Down function and Software Safety Stop flow diagram.



End of the document