CTAO System Control Concept

Doc. No: CTA-TRE-SEI-000000-0016-1a

05 October 2022

	First/Last Name, Organisation, Role	Digital signature
Prepared by (1)	E. Antolini, CTAO, System Control Coordinator	Elisa Antolini Digitally signed by Elisa Antolini Date: 2022.10.18 15:57:49 +02'00'
Prepared by (2)	G. Tosti, University of Perugia	Gino Tosti Firmato digitalmente da Gino Tosti Data: 2022.10.18 17:01:37 +02'00'
Approved by	N. Whyborn, CTAO, Lead Systems Engineer	Digitally signed by Nick Whyborn Date: 2022.10.19 09:43:06 +02'00'
Released by	W. Wild, CTAO, Project Manager	Wolfgang Wild Digitally signed by Wolfgang Wild Date: 2022.10.31 14:02:26 +01'00'

Revision History				
Issue	**Rev.**	**Created**	**Reasons / Remarks / Section**	**Author**
1	a Draft01	2020.01.29	First creation[1]	G. Tosti
1	a Draft01	2020.11.04	Included comments by Elisa, Vanessa, Igor, Nick.	G. Tosti
1	a Draft02	2021.12.15	Extended content and added comments based on the review process.	E. Antolini
1	a Draft03	2022.01.27	Included comments based on the II iteration of the review.	E. Antolini
1	a Draft04	2022.07.04	Included IKC comments.	E. Antolini
1	a	2022.10.05	Final version agreed with the IKC teams	E. Antolini

Authors	
First/Last Name, Organisation	**Contribution Subject/Chapter**
E. Antolini, CTAO PO	Producer of the document
G. Tosti, CTAO PO	Producer of the document
M. Gaug, CTAO PO	Contribution on Environmental and Calibration systems description

Abbreviations	
ACADA	Array Control and Data Acquisition
AECS	Array Element Control System
AIV	Assembly Integration and Verification
AIT	Assembly Integration and Test
BIT	Built in Test
CCD	Charge-Coupled Device
CTA	Cherenkov Telescope Array
CTAO-N	Cherenkov Telescope Array North site
CTAO-S	Cherenkov Telescope Array South site
CTAO-X	Cherenkov Telescope Array North or South site
CTAO	Cherenkov Telescope Array Observatory
FPGA	Field Programmable Gate Arrays
FRAM	F/Photometric Robotic Atmospheric Monitor
HMI	Human Machine Interface
IAC	Instituto de Astrofisica de Canarias
ICD	Interface Control Document
ICT	Information and Communication Technology
I/O	Input/Output
IPS	Integrated Protection System
LCS	Local Control System
LCU	Local Control Unit

[1] Created based on another drafted document “Control System Standard and development Guideline” SYS-STAND/310818, v. 0.4, prepared by Gino et. al. in 2018.

LST	Large-Size Telescope
MST	Medium-Size Telescope
OPC-UA	Open Platform Communication Unified Architecture
ORM	Roque de los Muchachos Observatory
PLC	Programmable Logical Controller
SCADA	Supervisory Control and Data Acquisition
SoS	System of Systems
SST	Small-Size Telescope

Table of Contents

1 Introduction 6
1.1 Scope 6
1.2 Reference documents 7
2 CTAO System- Level Control Concept 8
2.1 CTAO Controllers 9
2.1.1 ACADA 9
2.1.2 IPS 10
2.2 Technical Operations 11
2.2.1 Maintenance HMIs 11
2.2.2 Engineering HMIs 11
2.2.3 ACADA Technical Operations 12
2.3 Control Access Modes 12
2.4 Self-Recovery 13
2.5 Controllable Items 13
2.5.1 Monitoring and Logging 14
2.5.2 Control 15
2.5.3 Display 16
2.5.4 State Machine 17
2.5.5 Machine State 18
2.6 The Systems Control Hierarchy 19
3 Array Elements Control Systems 20
3.1 Control Hierarchy 22
3.2 CTAO-X Control Systems Deployment 23
3.3 Array Element Control System Standards 25
3.3.1 Communication Interfaces 25
3.3.1 Platforms and Languages 26
3.4 Time and Synchronization 26
3.5 Interlocks and Safety 26
3.6 Array Element Local Control Systems 27
3.6.1 Control and Safety Units 29
4 Definitions 30

Index of Figures

Figure 1 Main logical blocks of CTAO-X (X = North or South site) Control systems. ACADA manages the control functions (blue line) and provides the service for monitoring and display of the non-safety related parameters (blue dashed lines) of the controllable items. The IPS takes care of the site interlocks and safety and security functions of the controllable items (orange line), together with the acquisition and display of the safety-related parameters of the controllable items (orange dotted lines). 8
Figure 2 Machine State and Access Modes permitted transitions. 19
Figure 3 - The CTAO-X (X = North or South site) control systems hierarchy for the Controllable item. The " System" Manager in the level 2must be referred to any specific controllable item(e.g. for array element category is "Array Element Manager") 20
Figure 4- Generic Array Element decomposition for Complex Systems. 22
Figure 5 – The CTAO-X (X = North or South site) control systems hierarchy. Each Array element Control system include also a Array Element Interlocks and Safety system not represented in the figure. Azimuth motors and encoders are examples of field devices 23
Figure 6- General Topology of the CTAO-X (X = North or South site) Network infrastructure 24
Figure 7 - Deployment view of the CTAO-X (X = North or South site) System Control components. The System supervisors can be deployed also under the Array Element 25
Figure 8 General layout of the CTAO-X (X = North or South site) Array Element Control Systems internal/external communication interfaces. 26
Figure 9 - Representation of a general control structure. Here the controller is what in this document is called "Control Unit" 28
Figure 10- The generic architecture of an LCS 29

Index of Tables

Table 1 – Main technical features for Monitoring service. 14
Table 2 - Main technical features for Control service 16
Table 3 - Main technical features for Display service. 17
Table 4 - Combination of Access Modes and Power Status in the defined Machine States. 18

1 Introduction

The Cherenkov Telescope Array Observatory (CTAO) observing sites are located at the Instituto de Astrofisica de Canarias (IAC), Roque de los Muchachos Observatory (ORM) in La Palma, Spain in the Northern Hemisphere (CTAO-N) and close to the European Southern Observatory (ESO) Paranal site in Chile in the Southern Hemisphere (CTAO-S).

CTAO-N and CTAO-S (hereafter CTAO-X, where X can equally be N or S) are *System of Systems* (SoS) and as such has many layers of parts and behaviors that require control and integration.

CTAO-X SoS comprises several independent *Systems* with different level of complexity, comprising various internal sub-systems that includes several devices dedicated to specialized tasks (e.g. motion controllers, conditioning systems, safety guards, etc), which must be fully integrated into the CTAO-X to meet system requirements in terms of operation, performance, reliability, and maintainability.

Since the systems are provided by several suppliers without coordination may eventually lead to multiple solutions for the same problem, making it difficult for CTAO to update and efficiently maintain these systems, it is important to have a common reference framework for the development of the control of CTAO systems.

1.1 Scope

The scope of this document is to describe the concept and conventions adopted by CTAO for the realization of the control systems to be installed at both observation sites.

The approach described in this document must be applied to every supplier in charge to develop a control system belonging to CTAO-X, to minimize the CTAO life cycle costs, reduce both maintenance and logistic efforts, and keep the operational environment highly safe.

The intended audience of this document are systems engineers, designers, and developers in charge to provide any control system required by CTAO.

This document shall evolve as needed to reflect the final design of the control systems considered here.

For the scope of this document the CTAO-X SoS is composed of controllers and controllable systems (or controllable items), intended as defined in Section 4.

The content of this document refers to the involved systems as level B products, deeper levels of detail are not considered. In particular, for the Telescopes, we are not considering the separation between the Structure and Camera sub-systems and we are not giving any design specification for the lower level of control.

1.2 Reference documents

RD-1 CTAO Control System Standards, CTA-STD-SEI-000000-0004, Issue 1, Rev. a (draft02), 2022

RD-2 ACADA Architecture Design Document, CTA-TRE-COM-303000 0001, Issue 2, Rev. h, 2021

RD-3 CTAO Integrated Protection System Concept and Architecture (TBWritten)[2]

RD-4 CTAO Product Safety Plan, CTA-PLA-SEI-00000-0001, Issue 1, Rev a, 2020

RD-5 CTAO System Control Development Guidelines, CTA-TRE-SEI-000000-0017, Issue 1, Rev. a (draft03), 2022

RD-6 SST Telescope Architecture and Design Summary Report, SST-PRO-DSR-002, v1.0.

RD-7 CTA-N MST Requirement Spec. O. Schnurr Doc. No. CTA-SPE-SEI-306000-0001

RD-8 LST Technical Design Report, LST-TDR-140408, v4.2, 20190405

RD-9 Calibration Concept for CTA North, CTA-TRE-SEI-308000-0001, Issue 1.1, 2020-10-14

RD-10 Environmental Monitoring Concept for CTA-North, CTA-TRE-SEI-309000-0001, Issue 0.5, 2020-06-12

RD-11 Requirement Specification for On-Site ICT North, CTA-SPE-COM-302000 Issue 3, Rev. a, 19.04.2020

RD-12 Array Cock System: Architecture Design Document, CTA-TRE-COM-016000-0001 (In preparation).

RD-13 CTAO Alarm System (In preparation).

RD-14 Interface Control Document for ACADA – Array Element Monitoring, CTA-ICD-SEI-000000-0004 Issue 1, Rev. b, 2021

RD-15 General Electrical Design Specification, CTA-SPE-ELE-414000-0001 (In Prep.)

RD-16 Computing – On-Site ICT: IP-Structure CTA-SPE-COM-002000-0001, Issue 1, Rev.

RD-17 CTA Glossary at Jama

[2] Some aspects of IPS are still under discussion.

2 CTAO System- Level Control Concept

This Section aims to describe the concept of the system-level control adopted for CTAO.

As a system of systems, CTAO-X (where X can equally be N for North site or S for South site) contains several systems that are scattered over some squared kilometres and that need to be safely coordinated and monitored. Therefore, the CTAO-X Control system is a highly distributed control system containing a supervisory level of control overseeing multiple, integrated systems that are responsible for controlling the details of a localized equipment and processes.

Each CTAO site is provided by two central controllers, the *Array Control and Data Acquisition* (ACADA) [RD-2] and the *Integrated Protection System* (IPS) [RD-3], which interact with the following on-site *controllable items* represented as Level B products (see Figure 1):

- Small Size Telescopes[RD-6], Medium Size Telescopes [RD-7], Large Size Telescopes [RD-8] (Cherenkov Telescopes)
- LIDAR, FRAM, WS, Illuminators, Dust Monitor, Ceilometer, All Sky Camera (Array Calibration and Environmental Systems [RD-9][RD-10])
- Power Distribution System [RD-15]
- On-Site ICT Infrastructure [RD-11]
- Array Clock System [RD-12]
- Civil Infrastructure [TBWritten]

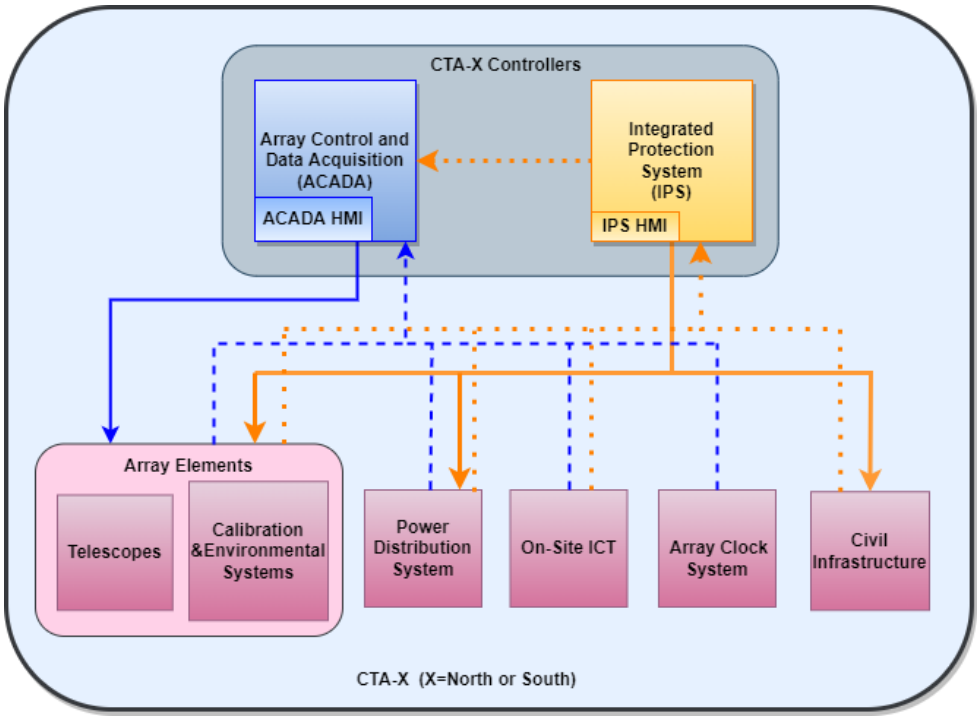

Figure 1 Main logical blocks of CTAO-X (X = North or South site) Control systems. ACADA manages the control functions (blue line) and provides the service for monitoring and display of the non-safety related parameters (blue dashed lines) of the controllable items. The IPS takes care of the site interlocks and safety and security functions of the controllable items (orange line), together with the acquisition and display of the safety-related parameters of the controllable items (orange dotted lines).

In the CTAO systems control, every controllable item (as defined in Section 4) is conceived as a stand-alone, independent, and active machine, able to perform autonomously all the required scientific and technical operations according to the received commands, as well as to transmit monitoring information and eventually recover from errors (see Section 2.4).

In this sense, every controllable item must be able to interact with the central controllers (ACADA and IPS), respecting the defined functionalities and the required technical specifications.

2.1 CTAO Controllers

As depicted in Figure 1, ACADA provide the service for the control, monitoring and display of the *non-safety related parameters* of the CTAO controllable items, while the IPS is the centralized system able to manage the safety and security aspects of the controllable items by triggering actions to the controllable items and acquiring and display the *safety-related parameters*.

Guidelines for the realization of the controllers, based on the given standard can be found in [RD-5].

2.1.1 ACADA

ACADA is the central highly reliable and fault-tolerant SCADA system of the controllable instrumentation, provided for each site of the observatory and realized as customized software product [RD-2].

ACADA interacts with the controllable items providing the following functionalities:

- Enable CTAO to operate simultaneously sub-arrays for scientific and remote technical operations (see 3.1.3), by controlling the Array Elements.
- Monitoring (acquisition and storage) service for the non-safety related parameters (including technical data) of Array Elements, ICT, Power Distribution System and Array Clock System, including the generation of non-safety related alarms of these systems [RD-13].
- ACADA HMI provides the service for the graphical interfaces used by the site operators to control and monitor the main operation process involving all monitored controllable items. Only the *non-safety related parameters* of the monitored controllable items that are critical for operations are displayed by ACADA.
- Support the AIV, technical, calibration and troubleshooting activities through scripts and command-line tools.

ACADA interact with IPS to:

- Receive the safety-related information (e.g. notification about the activation of interlocks and safety functions) from any system installed at CTAO-X.
- Provide the storage service for the safety-related parameters of the controllable items and the non-safety related parameters dedicated to the engineering and maintenance purposes of IPS (if any).

2.1.2 IPS

IPS [RD-3] is an independent system, implemented as integration of industrial solutions, dedicated to the protection of site assets. The IPS deals with all hardware, software and communication devices needed to ensure the safety and security of every observation site, in the sense defined in [RD-4].

The Safety category is related to the management of the hazards caused by malfunction of the machines as well as the external threats (e.g. bad weather, earthquake).

The Security aspect is dedicated to detection and prevention of unauthorized access, and access control, together with the protection of individuals and properties against external threats that are likely to cause harm,

The safety aspect is enabled in potentially dangerous machinery to protect people and the environment, while the security protects the machine to ensure that people cannot affect intentionally or unintentionally or even 'switch off' relevant safety functions. The safety and security aspects are not mutually exclusive, so they must work together and independently to guarantee that all the aspects are always covered.

Since every instrument is conceived as a stand-alone machine, every system overseen by the IPS must develop its protection measures to manage itself the actions to do in case of safety hazards. These systems must be developed following the standard provided by [RD-1] and designed to be technically compatible for the integration with the IPS.

IPS takes care of the site *interlocks* and *safety functions* of the observatory and interact with the individual safety and security systems installed in each product at that site [RD-3] to guarantee the following services:

- Manage the safety functions and triggering action on Array Elements and Power Distribution System.
- Manage the Security functions and triggering action on Civil Infrastructure, Array Elements and ICT.
- Acquire Safety-related parameters from all the controllable items having a local safety system (Array Clock System does not have safety equipment) to check and generate Safety-related Alarms.
- IPS-HMI displays to the operator the safety-related parameters and safety-related Alarms, critical for the operations.
- Possibility to locally store critical safety-related parameters (under definition).

IPS interact with ACADA to:

- Store the safety-related parameters acquired by the controllable items
- Share information useful to guarantee the safety and security aspects of the operations.
- Acquire and store the IPS parameters related to engineering and maintenance purposes (not critical for the operations).

2.2 Technical Operations

The *Technical Operations* include the engineering, technical calibrations, and maintenance activities (see definitions in Section 4) that can be performed in every device installed in the CTAO observatory.

For the execution of the technical operations that can be performed by using controllers/tools, as well as for the commissioning AIV and AIT stages, the CTAO concept provides the presence of two kind of Human Machine Interfaces, based on the well- known Local or Remote access modes, and the support of the ACADA central controller:

- The *Maintenance HMIs*, permitted to be used to control the system locally.
- The *Engineering HMIs*, to perform remote technical operations related to the single system.
- ACADA, to perform remote parallel/single operations related to the *Array Elements*.

The number and type of the Maintenance and Engineering HMIs (defined in Section 4 and called Technical HMIs) can be customized as needed, as well as the provided functionalities. Every Technical HMI must be designed and developed based on the standards provided in [RD-1], respecting the communication protocols, runtime environments and programming languages.

For every system, the technical data, as well as the calibration data for non-scientific purposes, non-critical for operations will be monitored through ACADA (See 2.5.1) but displayed to the Expert Operators only through Technical HMIs.

The active Array Elements (e.g. LIDAR, Telescopes) are required to be stand-alone machines, and the functionalities the instrument must provide for technical operations should be designed in a way that they can be managed as much as possible on the same way through ACADA and the Technical HMIs, without any duplication of functionality.

2.2.1 Maintenance HMIs

Every control system product, including controllers and controllable items, must be provided with proper Maintenance HMIs, to allow the execution of the functionalities needed to support the maintenance of the instrument and eventually the commissioning stage, AIV and AIT stages.

The Maintenance HMIs will be operable only at the location of the instrument, and accessible only to the designated Expert Operator. Whenever the Maintenance HMIs are in use, the remote control of every device of the system must be fully detached (see Section 2.3 and Section 2.5.5). The monitoring of ACADA remains active.

Note

- The management of the control functions of IPS and the possibility to override the security and safety coverage (or part of it) during the Maintenance activities is still under definition.
- The scope of this document only includes level 1 maintenance.

2.2.2 Engineering HMIs

Every control system product, including controllers and controllable items, must be provided with proper Engineering HMIs, to allow the execution of the functionalities needed to support the

Engineering and technical calibration activities of the instrument, and eventually the commissioning, AIV and AIT stages.

The Engineering HMIs will be operable only remotely, and accessible only to the designated Expert Operator. Whenever the Engineering HMIs are in use in that system, no stuff must be present in the field and the remote control of ACADA (for the *Array Elements*) must be fully detached (see Section 2.3 and Section 2.5.5). The monitoring of ACADA remains active.

Remote Engineering operations will be done only through the onsite network.

Note

- The management of the control functions of IPS and the possibility to override the security and safety coverage (or part of it) during the engineering and technical calibration activities is still under definition.
- The possibility to perform remote engineering operation by using outside network is related to the risk analysis which is under development.
- Offsite engineering operation will be described in a TBWritten document.
- Security rules are under definition.
- How and where the Engineering HMIs are hosted is still under definition.
- The interaction of the Engineering HMIs with the different systems must be defined by the instrument experts.

2.2.3 ACADA Technical Operations

The *controllable items* managed by ACADA, have the possibility to execute some remote technical operations with the support of ACADA.

The idea is that ACADA, through the scripts environment or command line environment [RD-2], can command the engineering, calibration, and maintenance procedures, executed in parallel by more than one *Array Element*. Engineering and calibration procedures can also be performed by single instrument.

The actions executed in parallel can be applied only to the instruments belonging to the same category or a subset of it: SST Category, MST Category, LST category, LIDAR category and so on.

If the remote technical activities affect all the array elements, the ACADA system should be in the technical operation mode, where no scientific operations are possible. In the case of remote technical operations involving only a single instrument or a sub-set of it, for which scientific observations can be performed in parallel (using the other array elements) ACADA will be in the *Science* operation mode [RD-2], while still have array elements detached which are doing the technical operations.

2.3 Control Access Modes

For the scope of this document the access mode is considered the way to perform the control of an instrument/system, which is related to the position where the user/controller is located with respect the machine to be controlled.

The main access mode categories, to perform the scientific and technical operations of each instrument, are the *Local Access mode* and the *Remote Access mode*, as defined in Section 4.

Within these categories, the following access modes are defined for the CTAO systems control, based on the instruments considered (Array Element or not), the number of Array Elements involved, and the kind of operations to be performed (Scientific or Technical):

- **Remote Array,** *Remote Access Mode* applicable only to the Array Elements, when ACADA has the full control of the instrument for the Scientific operations executed remotely.
- **Remote Array Engineering,** *Remote Access Mode* applicable only to the Array Elements, when remote technical operations of the whole array, or a sub-set of it, are performed through ACADA.
- **Remote Stand-Alone Engineering (Remote Stand-Alone),** *Remote Access Mode* applicable for remote technical operation of a single instrument performed through the Engineering HMI. The ACADA control part is fully detached, and the monitoring is active.
- **Local Maintenance (Local)**, *Local Access Mode* applicable to execute maintenance operations of a single Instrument, performed through local Maintenance HMIs'. Any remote control is fully detached. The Monitoring from ACADA is active.

2.4 Self-Recovery

Every control system delivered for CTAO are expected to adopt the *self- recovery* concept to some critical categories of hardware and software errors defined in [RD-13], so that whatever applicable, the failure occurrence may be fixed by the system itself with no need for external intervention.

In this context Built In Test (BIT) and the related equipment, as well as the execution of self-diagnosis techniques, are required to be considered in designing the control system self-recovery procedures only after careful evaluation with value-added justification and considering priority on situation that can trigger potential safety hazards.

The BIT, self-diagnosis and potential self-recoveries techniques, if applied, must be properly included into the definition of the State Machine of the instrument.
Whenever possible, if the self-diagnosis/self-recovery of the system fails, there must be the possibility to restart/reboot the components, if possible remotely, through the Engineering HMIs. The instrument controlled by ACADA, must also develop the possibility to be restarted directly from ACADA.

Note
The self-recovery procedure is proposed to be applied only for some critical categories of HW and SW errors due to the very high cost of the implementation.

2.5 Controllable Items

In this Section will be provided a summary of the main technical features that every controllable item is required to follow to be integrated within the central controllers (ACADA and IPS) for monitoring, control, and display services.

The technical features will be presented in tables containing the following information:

- Main functionalities provided by the service (Functionality)
- The activities of the observatory where the service is active (Activity)

- The Access Modes for which the service is active (Access)
- The Controllers providing the service (Provided by)
- The communication protocol used for the service (Protocol)
- The Frequency rate required for the monitoring (Frequency Rate, only for Monitoring)

The Control Systems of the controllable items are required to be designed and developed following the CTAO standards and respecting the interfaces agreed with the controllers [RD-1].

Within the controllable items, the *Array Elements Control Systems* (AECS) are intended to be developed as customized solutions, to satisfy the required scientific functionalities. The control systems of the other elements are intended to be realized as integration of industrial solutions.

Guidelines for the realization of the controllable items based on the given standard can be found in [RD-5].

2.5.1 Monitoring and Logging

Table 1 summarizes the main technical features required for the monitoring services available for every CTAO controllable item.

Controllable Items	Functionality	Activity	Access	Provided by	Protocol	Frequency Rate
Array Elements (AE)	Acquire and Store parameters for scientific purposes	Scientific Operation	Remote Array	ACADA	OPC-UA ACS	TBD TBD
Array Elements Power Distribution System Array Clock System On-Site ICT	- Acquire and Store parameters for engineering/maintenance/calibration purposes. - Generate Non-safety related alarms/Error/warning. - Store Safety parameters.	All (except when Off)	All	ACADA	OPC-UA ACS (AE) Other (TBD)	
Array Elements Power Distribution System On-Site ICT	- Acquire parameters for Safety purposes. - Generate Safety - related Alarm/Error/Warnings. - Temporary storage of critical Safety-related parameters (if ACADA monitoring is not available).	All (except when Off)	All	IPS	OPC-UA	TBD

Table 1 – Main technical features for Monitoring service.

For the monitoring service ACADA provides an interface and a service to handle the data. The details are contained in the specifications of the ACADA sub-system dedicated to the monitoring.
The Logging service for the Array Elements will be provided by ACADA, trough the ACS and OPC-UA protocols. The logging service for the other controllable items is still under definition.

Notes
For the controllable items developed as industrial solutions the following aspects are under investigation:

- The protocol of the non-safety related parameters is meant to be the OPC-UA of ACADA. Whenever the OPC-UA protocol is not applicable for incompatibility with the chosen industrial solutions, then we will find out what other protocol can be available for the equipment of the system and eventually see if ACADA can support these protocols (e.g. Simple Network Management Protocol).
- The requirements for the acquisition rate of the non-safety related parameters will be calibrated based on the ACADA technical features, contained in the Monitoring ICD for the OPC-UA part [RD-14].
- We are checking if the frequency rates defined by ACADA are compatible with the industrial solutions selected. In that case the requirements for the acquisition rate of the non-safety related parameters will be calibrated based on the ACADA technical features, contained in the Monitoring ICD for the OPC-UA part [RD-14].
- If some systems will not be compatible with any protocols supported by ACADA for technical reasons, then we will introduce a tool for the real time acquisition of the parameters of these systems, possibly to be assimilate as part of another existing product.

2.5.2 Control

The general control activities of the controllable items which do not need to be controlled for the scientific operations through ACADA, are listed below and are mainly related to technical activities. The detailed functionalities will be reported in the related specification documents.

<u>Power Distribution System</u>

- Switch On-Off Relays/Main Disconnectors/UPS

<u>Array Clock System</u>

- Calibrate the system
- Switch On/Off components

<u>On-Site ICT</u>

- Manage/Calibrate/Restart/Switch On-Off:
    - Network Switches
    - Routers
    - Servers and PCs

Table 2 summarizes the main technical features required for the control services available for every CTAO controllable item

Controllable items	Functionalities	Activity	Access	Controlled by	Protocol
Array Elements	Coordinate the execution of the scientific procedures/functionalities.	Scientific Operation	Remote Array	ACADA	ACS
	Command the instruments to execute parallel engineering /calibration procedures	Parallel Engineering/ Calibration	Remote Array Engineering	ACADA	ACS
On-Site ICT (Except IPS) Array Elements Power Distribution System Array Clock System	Command the instruments for stand-alone engineering /calibration activities.	Stand-alone Engineering/ Calibration	Remote Stand-Alone	Engineering HMIs	OPC-UA (TBC)
	Command the instruments for stand-alone Maintenance activities.	Maintenance	Local	Maintenance HMIs	Internal
	Command the instrument to execute safety/emergency procedures (e.g. park the telescope, switch-off a component)	Emergency/ Safety	All (Except Local)	IPS	TBD

Table 2 - Main technical features for Control service.

Notes

- The IPS control service is not applicable for On-Site ICT equipment.
- The use of OPC-UA protocol for the Engineering HMIs needs to be confirmed.
- It is under investigation if the emergency/safety procedure can be managed only by IPS or through the Engineering/Maintenance HMIs.
- It is still under investigation if safety/security functions are active in Local access mode (see 3.2.1).
- The Safety-related aspects of the Dust Monitor, All Sky Camera and Illuminator are under discussion.

2.5.3 Display

Table 3 summarizes the main technical features required for the display service available for every CTAO controllable item.

Controllable items	Functionalities	Activity	Access	Displayed by
Array Elements only	Check status of parameters for scientific purposes	Scientific operations	Remote Array	ACADA HMI

Array Elements only	Check status of parameters for parallel engineering/calibration and maintenance purposes	Engineering/Calibration	Remote Array Engineering	ACADA HMI
Power Distribution System Time Synchronization System On-Site ICT Array Elements	Check status of Safety related Critical Parameters.	All (Except when Off)	All	IPS HMI
	Check status of Non-Safety related Critical Parameters	All (Except when Off)	All	ACADA HMI
	Check status of parameters for stand-alone engineering/calibration and maintenance purposes	Engineering/Calibration	Remote Stand-Alone	Engineering HMIs
		Maintenance	Local	Maintenance HMIs

Table 3 - Main technical features for Display service.

The protocols for the display part of the HMIs are part of the package and are intended to be defined internally and in the respect of the given standard for the development [RD-1].

2.5.4 State Machine

Every controllable item is conceived as an independent machine which must be able to be easily integrated into the central controllers and efficiently maintained for the whole lifetime of the observatory.

The products, realized as customized systems (e.g. telescopes) and/or with integrated industrial solutions, must adopt the *Deterministic Finite State Machine* approach in designing and developing the control part of the system, to efficiently be controlled, and execute the required functionalities in coordination with the other instruments.

The following rules must be considered:

- The state machine approach must be applied to every layer of control as defined in Section 2.6.
- The state machines of the system must be designed considering the integration between the different layers of control.
- The deterministic aspect of the system must be respected at every layer of control: undefined states and unknown configuration cannot be acceptable.
- Any possible configuration of the system, and the possible transitions between them, must be known at any time, and must be mapped to the appropriate well-defined states.
- The State Machines to be exposed to the central controllers (e.g. ACADA) for the control provided at *Manager Level* (see section 3.1) must be developed as agreed by the two parties, and efficiently integrated into the other layers of control.
- At the other levels of control, the number of states, the names, the state transitions, and the specific configurations can be customized as needed, as much as the deterministic aspect of the system is respected.

2.5.5 Machine State

Every controllable item that undergoes to the control systems standards, as specified in [RD-4], must adopt and implement the concept of the *Machine State*, as defined in this Section.

The definition of the *Machine State* must be intended for the purpose of CTAO, as the equivalent terminology to the *Operating Modes* described in the 2006/42/EC *Machine Directive* [RD-4], in the sense that each machine can have one or more operating mode determined by the type of machine and its application.

The *States* of the Machine States, defined for the purpose of CTAO consider a combination of the status of the power and the permitted access modes (defined in section 2.3) for the control of the instrument, as presented in Table 4. They are not intended to describe the internal configuration of the instrument.

	Access Modes				
Power Status	Machine States	Local Maintenance	Remote Stand-Alone	Remote Array	Remote Array Engineering
	Power - Off	OFF	OFF	OFF	OFF
	Power - ON	MAINTENANCE	ON	ON	ON

Table 4 - Combination of Access Modes and Power Status in the defined Machine States.

The configuration of the instrument in the different states is defined as follow:

- In OFF state the instrument is completely powered off and no control is possible.
- In ON state the instrument is powered-on and it can be controlled only remotely by ACADA (Remote Array Engineering or Remote Array) or by the Engineering HMIs (Remote Stand-Alone Engineering). No people are present on the field.
- In MAINTENANCE state the Expert Operators can power on/off the devices of the instrument. The control of the instrument can be possible only for local technical operations (Local Maintenance). This state also includes the power isolation procedure and the inhibition of the drive system (if needed).

The permitted state transitions are depicted in Figure 2, and must be performed and implemented based on the standard on machinery and in the respect of safety rules and procedures defined in [RD-4]. In particular:

- The transitions between the different states ON, OFF and MAINTENANCE must be triggered locally at the instrument.
- The Local Maintenance (MAINTENANCE) <-> *Remote Stand-Alone* (ON) access mode transition must be managed only locally at the instrument.
- By default, when entering from another state, the access mode for the ON state must be *Remote Stand-Alone.*
- Within ON state, the transitions between the different remote access modes must be managed through the HMI of ACADA.

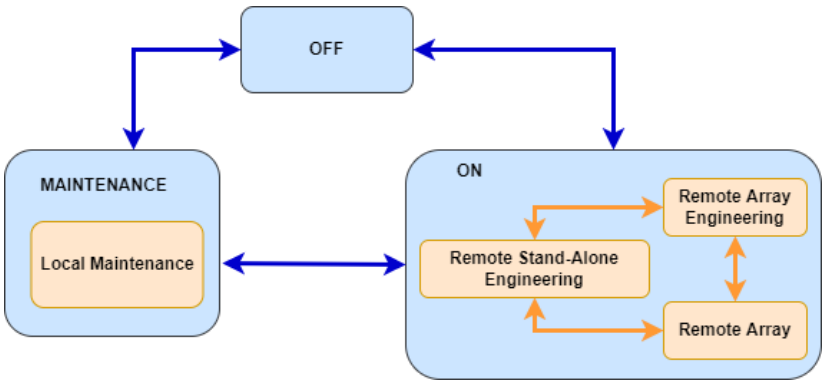

Figure 2 Machine State and Access Modes permitted transitions.

Notes

The implementation details, procedure and safety aspects are out of the scope of this document. The configuration of the instrument in the ON state must be defined in the related technical documentation (e.g. Telescope Generic State Machine).

The reference standards are:

- BS EN 60204-1:2018 (9.2.3.5 Operating modes).
- 2006/42/EC (1.2.5 Selection of control or operating modes).
- IEC 60204-1:2016 (Chapter 5, Isolation of the power).

2.6 The Systems Control Hierarchy

The control hierarchy should not be considered as a proposal of internal architecture for level B sub-systems, but it is a grouping into different levels of the hardware and software equipment dedicated to the control of the instruments.

The CTAO systems control hierarchy provides three basic levels of control, as depicted in Figure 3. Every level refers to the group of hardware and software equipment dedicated to different purposes in the control chain defined for CTAO.

Level 1 is occupied by the central controllers ACADA and IPS. At level 2 is located *the "System" Manager*, a software layer in charge to coordinate and manage the functionalities provided by the different sub-systems, and which interface directly with the controllers. Some controllable items may don't need to have this layer (e.g. Weather Station) or they can be bypassed for specific functionalities (e.g. IPS communication with the hardware, Monitoring). This layer of software, when present, must respect the interface and protocols agreed with the controllers and must take the name of the controllable item (e.g. Array Element Manager, Power System Manager, ICT Manager).

The third level is reserved to the *Local Control System* of the controllable items, indicated as a black box containing hardware and software equipment belonging to *control* and *safety unit(s)*, devices and local communication infrastructure required to guarantee safely functional operation, verification, and maintenance activities of the instrument.

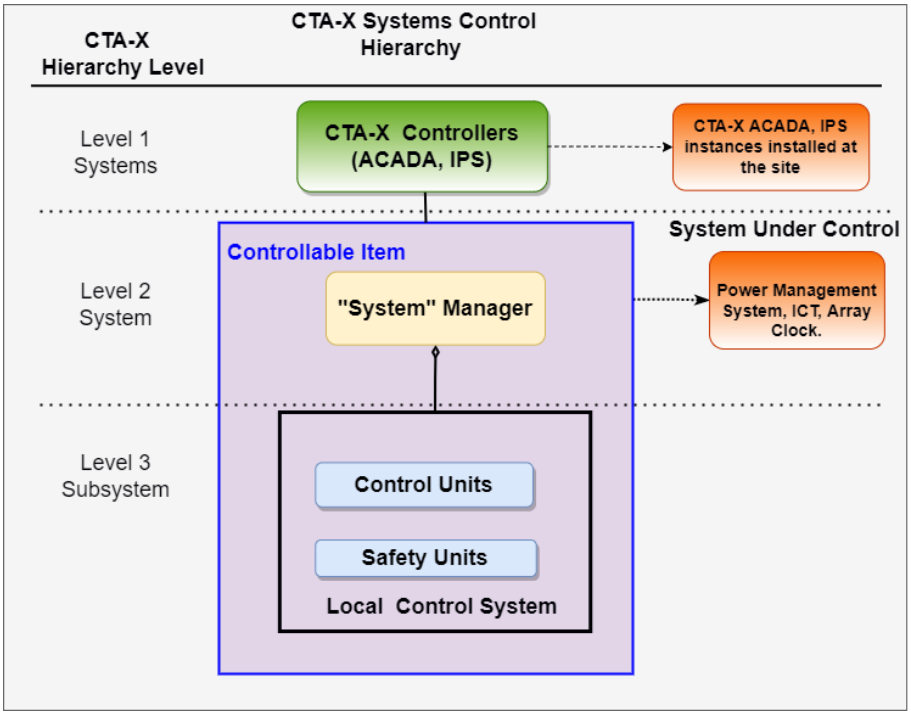

Figure 3 - The CTAO-X (X = North or South site) control systems hierarchy for the Controllable item. The " System" Manager in the level 2must be referred to any specific controllable item(e.g. for array element category is "Array Element Manager").

Additional levels of control are provided only for the most complex *Array Elements* (e.g. Telescopes), which must support motion functionalities, and which architecture follows a functional decomposition close to its physical hardware hierarchical decomposition. For these systems, at the lowest level, the control of the processes is usually achieved by using feedback or feed-forward control loops to automatically maintain key process conditions around a desired set point. See Section 3 for more details.

Any additional layer for the controllable items developed as industrial solutions or an integration of different industrial solutions (Power distribution system, ICT and Array Clock Systems), must be managed and designed internally by the systems.

For stand-alone Engineering and maintenance operations, each level of control can be equipped with the Maintenance and Engineering HMIs, based on the needs of the product, taking into account the principle to avoid duplication of functionality (see Section 2.2).

3 Array Elements Control Systems

The Array Elements Control Systems (AECS) are the most complicated control systems to be developed as customized solutions for CTAO. These systems are conceived as stand-alone machine in charge to develop their own safety and non-safety functionalities that must be integrated with ACADA and IPS. For this reason, is important that every AECS is designed following the technical features and control hierarchy provided in this section, to be compatible with the architectures and interfaces of the central controllers.

The CTAO *Array Elements* are:

- The Cherenkov Telescopes, which include three different types of Telescopes:
  - The Large-Size Telescope (LST)
  - The Medium-Size Telescope (MST)
  - The Small-Size telescope (SST)
- The Environmental Monitoring and Calibration Systems:
  - Raman Lidar: system used to characterize atmospheric aerosol extinction from ground to about 20 km a.s.l.
  - FRAM (F/Photometric Robotic Atmospheric Monitor) device, which is a small robotic astronomical telescope with a large field of view and a sensitive CCD camera using stellar photometry to measure atmospheric extinction.
  - Weather Stations
  - Dust Monitor: system measuring the density of dust particles in separate size bins
  - Ceilometer: system to measure cloud altitudes and thicknesses
  - Illuminator: system to illuminate an individual telescope with pulsed light at different wavelengths and intensities.
  - All Sky Camera: a calibrated camera with a 2π-field-of-view used to measure aerosol extinction across the whole observable sky.

Between the Array Elements, the *Telescopes Control System* (which apply to all the SSTs, MSTs and LSTs), the *LIDAR Control System* and the *FRAM control system are the* the most complex to design and the related technical specifications are treated in this section (TBD with Markus if Ceilometer, illuminator need complex customized solutions for control system).

These three AECS must provide common functionalities (e.g. move mechanical structures to point detectors field of view toward a predefined sky location, alignment of optical elements, photons detections and signal readout, etc.) implemented with different technological solutions that consider the different degree of complexity need to satisfy the user and performances requirements specific to the scope for which the system is designed. However, from the point of view of the Control System design, telescopes, Lidars and FRAM have several commonalities and then a common logical Architecture can be used for all of them. Figure 4 shows a common logical blocks decomposition to applicable to each of these systems and that can be used to derive common control system design patterns.

The Mount subsystem includes the hardware and software responsible of the pointing of the Array Element to different parts of the sky.

The Optical Elements subsystem includes the hardware, software, and communication devices responsible for the light signal collection and delivery to the Camera. The optical elements are generally mounted on the Mount subsystems.

The Camera subsystem includes the hardware, software, and communication devices responsible for the light detection, signal conditioning and readout. For the scope of this document a camera can be a Cherenkov Camera, a Charge-Coupled Device (CCD) Camera or a photometer. The Camera is generally mounted on the Mount subsystems.

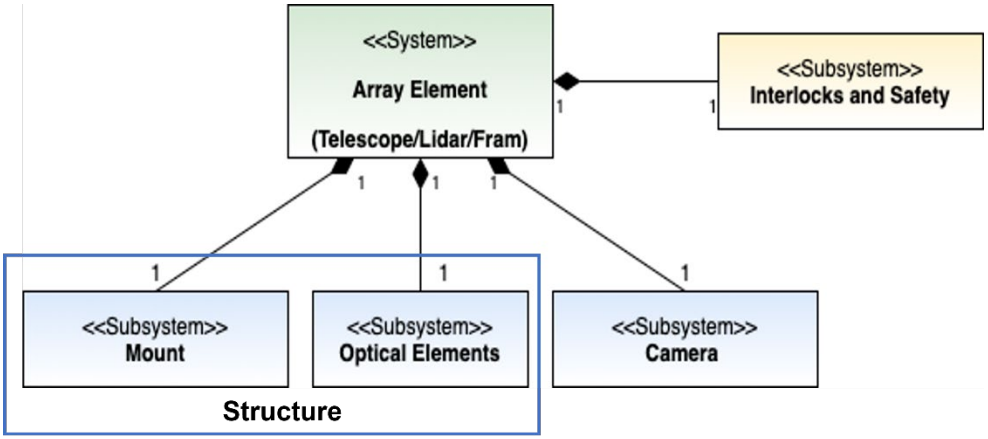

Figure 4- Generic Array Element decomposition for Complex Systems.

3.1 Control Hierarchy

Figure 5 shows a graphical representation of the hierarchical levels of the CTAO-X *Array Elements* control systems towards ACADA. The connection with IPS is intended to be direct, so no hierarchy is needed to be shown for IPS in this document.

Every level refers to the group of hardware and software equipment of the Array Element, dedicated to different purposes in the chain defined for the control of ACADA. The Local Control System is shown as a black box in which the two hierarchy levels are not mapped with any of the sub-systems defined for the instrument.

Whenever required, the AECS must develop an *Array Element Manager* software component, implementing management and coordination functions of the sub-systems, controlled at lower level by the *Local Control Systems*, and providing direct connection toward ACADA. The following Managers must be provided and implemented based on the standards given in [RD-1]:

- Telescope Managers
- LIDAR Managers
- FRAM Managers
- Others (TBD)

The Managers related to the sub-system of each instrument are not specified in this document and are intended to be part of the related Manager. In the case of the Telescope, the Camera and Structure Managers are included in the Telescope Managers.

Each Local control System is equipped with several *Supervisors* that allow safety, control and maintenance of its sub-systems (e.g. the Structure of a Telescope). Each Supervisor provide the interfaces responsible of the control and safely operations of the field devices (actuators and sensors). Furthermore, the AECS includes its own Interlocks and Safety system, not represented in.

The generic architecture of a *Local Control System* of an Array Element and the functional description of its subsystems is given in Section 3.6 to enforce a common language, concepts, and development process, and then, increase the operation and maintenance efficiency due to the possible commonalities that can be shared between different *Array Elements*.

The interfaces between Array Element Control System and the central controllers (ACADA, IPS) are defined in the related Interface Control Documents (ICDs) specifying command, alarms, monitoring data types, formats and rates and characteristics of the data communication.

The Array Element Managers and the related Local Control Systems are delivered by the CTAO supplier and then integrated into the central controllers.

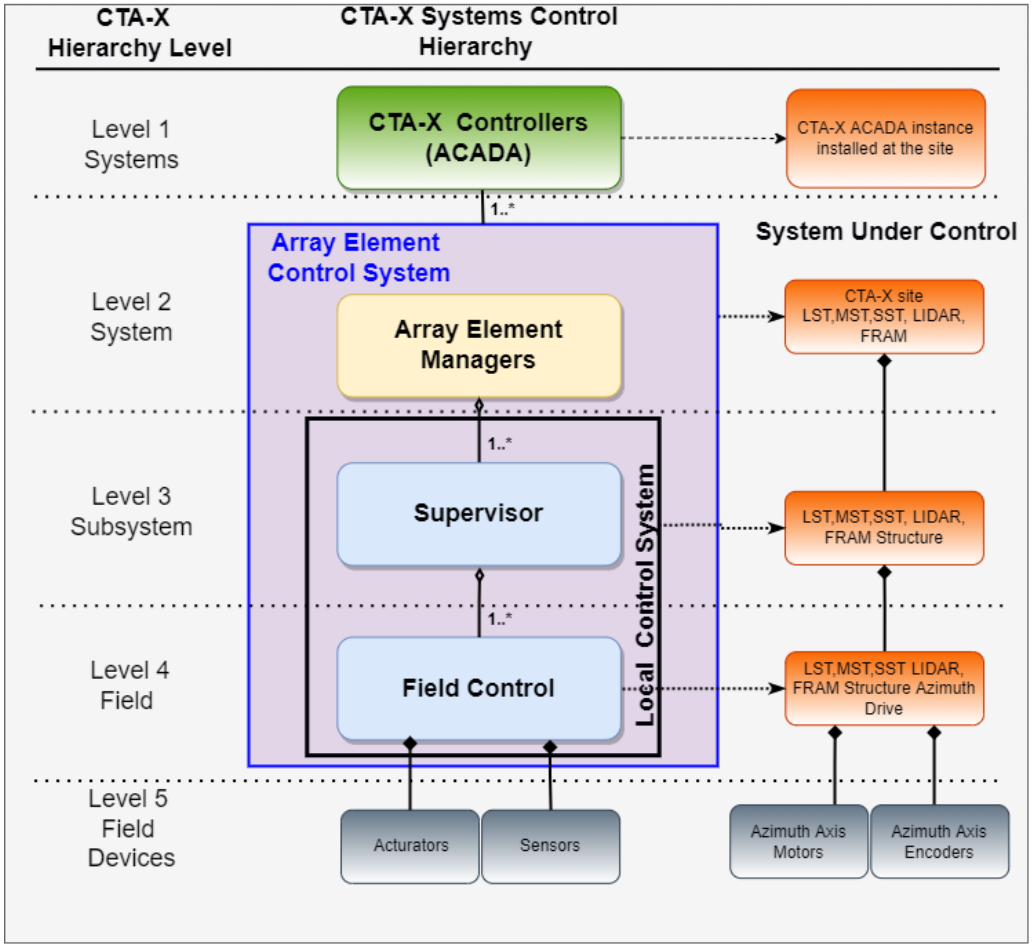

Figure 5 – The CTAO-X (X = North or South site) control systems hierarchy. Each Array element Control system include also a Array Element Interlocks and Safety system not represented in the figure. Azimuth motors and encoders are examples of field devices.

3.2 CTAO-X Control Systems Deployment

At the CTAO-X sites the *Array elements* are physically distributed over an area of several square kilometres. For the scope of this document, the physical deployment of the CTAO-X Systems Control will be considered over three main locations:

- The Array Elements area, in proximity of the Telescope structure or of an Environmental Monitoring and Calibration system equipment.
- The On-Site Control Room.
- The On-Site Data Centre.

These areas are connected by a networking infrastructure schematically represented in Figure 6. A detailed description of the CTAO-X network infrastructure is given in [RD-11][RD-16].

The field electronics (the hardware components interfacing with sensors and actuators) should be installed in the *Array Elements* areas, while the Field controls can be installed in the *Array Elements* areas or in the On-Site Data Centre, depending on the performance and safety requirements of each specific application.

The AE Managers should be installed at the data center and shall use the CTAO defined and provided hardware according to an approved ICD with onsite ICT. The supervisors can be deployed at the array element or in the data center.

All the hardware and software components of the control system installed in the *Array Elements* areas must interface to the CTAO-X Service Cabinet providing standard connection to the electric power, data, safety and time networks.

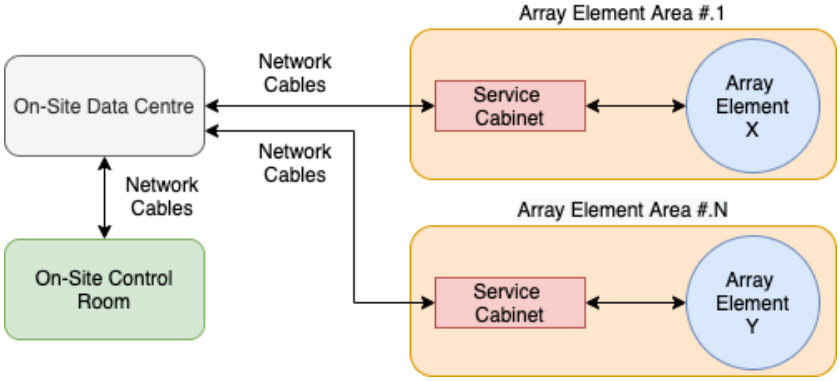

Figure 6- General Topology of the CTAO-X (X = North or South site) Network infrastructure

Each CTAO-X site has a Data Centre providing all networking and computing services. All network cables starting at the service cabinet serving the *Array Elements* areas will terminate in the On-Site Data Centre where they can be connected to *Array Elements* specific control system equipment.

General information related to the interfaces of the Array Elements with the service cabinet, On-site Data Centre and its interfaces with the service cabinet are contained in [TBWritten].

The On-Site Control Room includes terminals to display operation and engineering panels for the CTAO-X control systems. The On-site Control Room and its use cases are described in [TBWritten].

Figure 7 shows a deployment view of the CTAO systems control components.

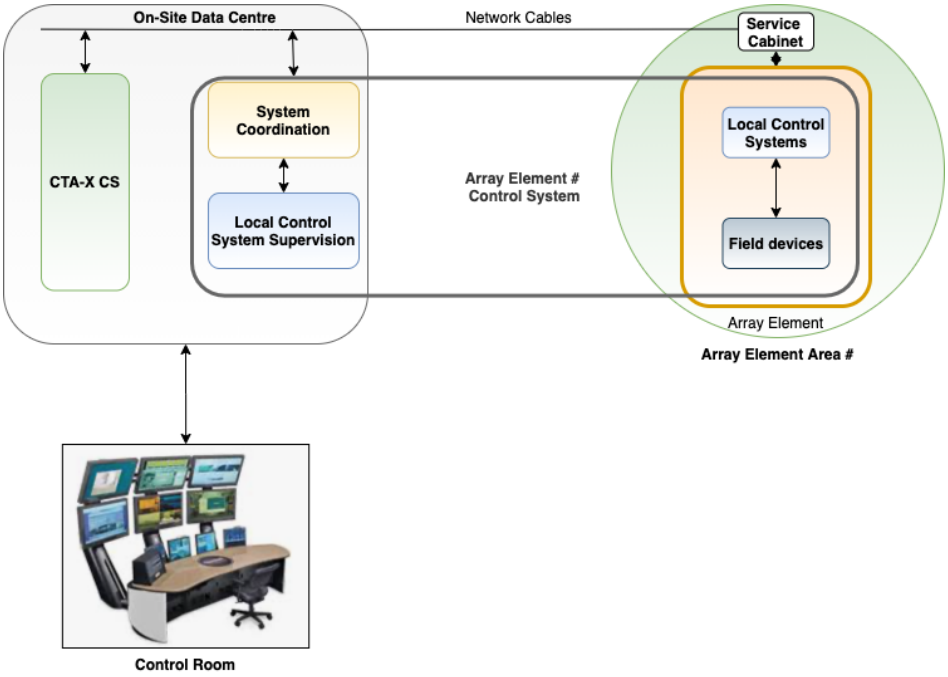

Figure 7 - Deployment view of the CTAO-X (X = North or South site) System Control components. The System supervisors can be deployed also under the Array Element.

3.3 Array Element Control System Standards

The baseline standards to be used for construction of the CTAO-X Array Element Control Systems are given in [RD-1]. The main driver principles for those standards are briefly reported in this Section.

3.3.1 Communication Interfaces

A graphical representation of the internal and external networking communication interfaces of an Array Element Control System is reported in Figure 8.

The *Data Network (External)* is referring to the data flow interacting towards ACADA and which interfaces with the Array Element Mangers (by using ACS middleware) and the Supervisors (by using OPC-UA or others agreed upon protocols) including the following data stream:

- Control commands from ACADA
- Monitoring Data, including Scientific Data, Technical Data, Calibration Data, Logging Data and Housekeeping Data.

The *Control Network* refers to the control data stream managed internally by each Array Element, which provides connection for the management of the different field controls by the Supervisors, including the internal fieldbus connections.

The Safety Network represents the Safety-related parameters data stream towards IPS (including Alarms), coming directly from the field devices and the related Field Controls.

The Time Distributions Network contains the data stream for the time synchronization of the Array Elements with the centra clock. See Section 3.4 for more details.

The protocols of these communication interfaces follow the standards given in [RD-1]..

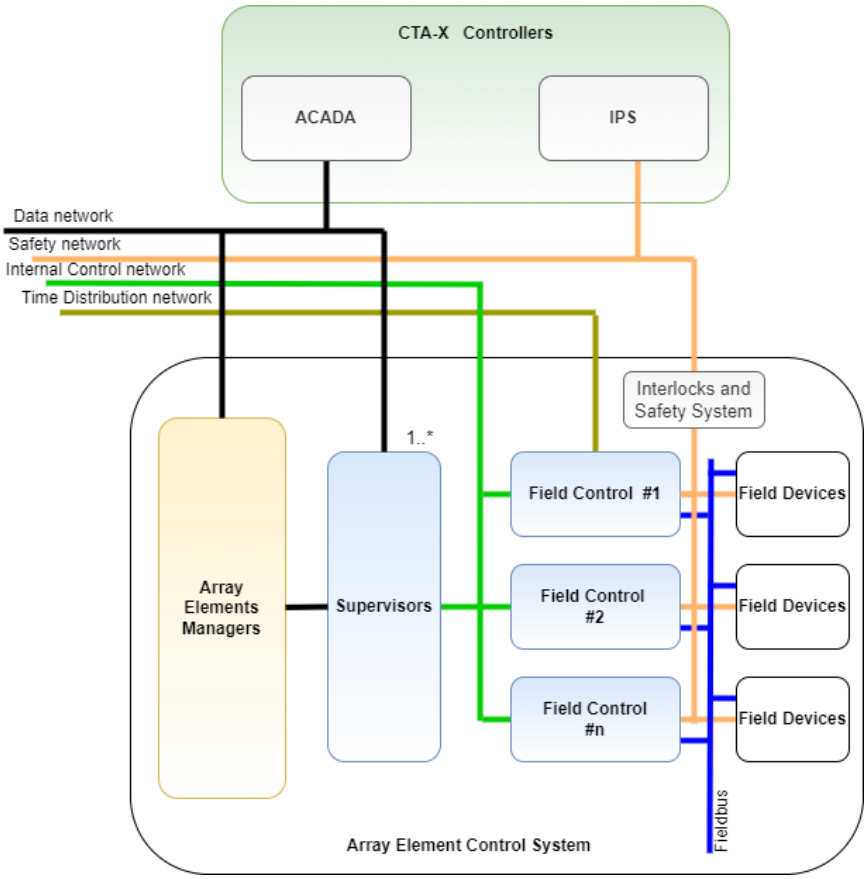

Figure 8 General layout of the CTAO-X (X = North or South site) Array Element Control Systems internal/external communication interfaces.

3.3.1 Platforms and Languages

The standard for the set of the hardware platforms, software languages and development environments required to build Array Elements Control System is given in [RD-1].

3.4 Time and Synchronization

At each CTAO site the network infrastructure provides to the CTAO-X distributed control systems, time synchronization via the CTAO-X site Master Clock [RD-12].

3.5 Interlocks and Safety

The Interlock and Safety system of the Array Element can be seen as a hierarchical system of Local Interlock and Safety equipment responsible for subsystem level safety, and the integration of these Local systems in the IPS parts responsible for CTAO-X level safety.

The Array Element Interlock and Safety System must implement the logic ensuring integrity of the equipment and personnel.

The design of the Safety Units and the related safety functions must follow the safety standards

provided by CTAO [RD-1]. In particular only safety functions presented in the EN ISO 13849-1 standard will be accepted.
The CTAO safety policy is based on the adoption of the functional safety approach described in [RD-1], and imposes that a control unit (e.g. PLC) used for safety related functions is accepted only if it is safety certified and reaches SIL 2 or SIL 3. Safety PLC is an example of a Local Safety Unit (see Section 3.6.1) that benefits of a traditional PLC system to replace the hard-wired relay systems normally required to bring automated processes to a safe state. The safe state intended here is as defined in the functional safety IEC 61508, and it is referred to the action of the Local Safety Unit: The state of the process after acting to remove the hazard resulting in no significant harm. It means the instrument should be in a safe state with respect the hazards that have been occurred.

Electromechanical components used for safety functions as inputs (i.e. sensors) or outputs (i.e. actuators) shall be safety certified and reach a SIL 2 or 3, even if they are new build/design or Commercial Off-the-Shelf (COTS) items. Guidelines for the development of the Safety System are available in [RD-5].

CTAO-X Array Elements equipment shall follow the requirements of the directive on machinery as defined in [RD-1]. Furthermore, motor drive systems with integrated safety functions shall be used for the telescope's motion in both axis (azimuth and elevation). The functions within the drive itself shall provide effective protection for personnel and machinery. The connection of the drive to a safe fieldbus provides safe decentralized I/Os, reduces engineering development work and minimize certification expenses.

The Product Safety Plan [RD-4] formalizes the requirements for the Product Safety analysis and risk reduction activities that shall support the detailed design of any Array Element.

For the required calculations, such as failure rate and reliability, information has to be collected from suppliers for specific components or using failure rate from similar applications from the past experience or specialized prediction software (e.g. Reliasoft).

Guidelines for the development of the Safety Units and Safety functions are available in [RD-5].

3.6 Array Element Local Control Systems

Each Subsystem of an Array element may include multiple *Local Control Systems* which control the field devices.

The scope of a control system is to obtain a well-defined and quantified output from the controlled physical system, in spite of the interaction with the environment that is a source of disturbances (see Figure 9).

For achieving this purpose two main classes of devices are used: *actuators* which convert control commands into physical effects (e.g. a motor driving a pointing system based on the values of the input current), and *sensors* which measure states of the controlled physical system and provide control feedback to the controller.

The *controller* can range from something very simple, such as an ON/ OFF logic, to a highly complex system that includes functions for selecting different control modes, monitoring of physical system parameters and status, failure detection isolation and recovery, etc.

The Programmable Logic Controllers (PLC), a computer-based device, is one of the most used type of controller in industrial and scientific applications.

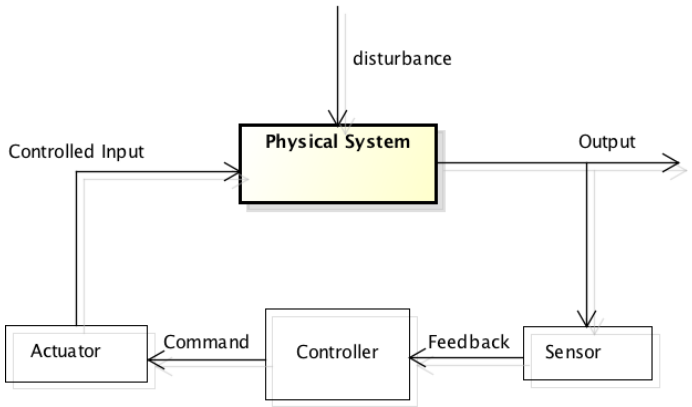

Figure 9 - Representation of a general control structure. Here the controller is what in this document is called "Control Unit"

An LCS may contains the control and safety logic unit(s), devices and fail-safe communication infrastructure to preserve the required integrity of the associated items and guarantee human safety.

An LCS of an Array Element shall have the following properties.

- The interfaces provided by the LCS shall be limited to the domain of the LCS components, making no constraint or assumption about other Array elements subsystems.
- The execution of the functions provided by the LCS shall not create a hazardous situation.
- The LCS interfaces to the actuators and sensors of the field devices.
- The LCS controls individually and independently any equipment (e.g. brakes, circuit breakers, shutters, valves, etc.) of the field devices.
- The LCS controls individually and independently any function (e.g. position control, power control, etc.) of the field devices.
- In an LCS there shall be no execution coupling between control and safety functions
- The safety functions should be executed by safety certified equipment.

Figure 10 shows the generic architecture of an LCS. In some special case an LCS can consist of only one or more Local Control Unit (LCU) and the Local Safety Unit (LSU) could not be present.

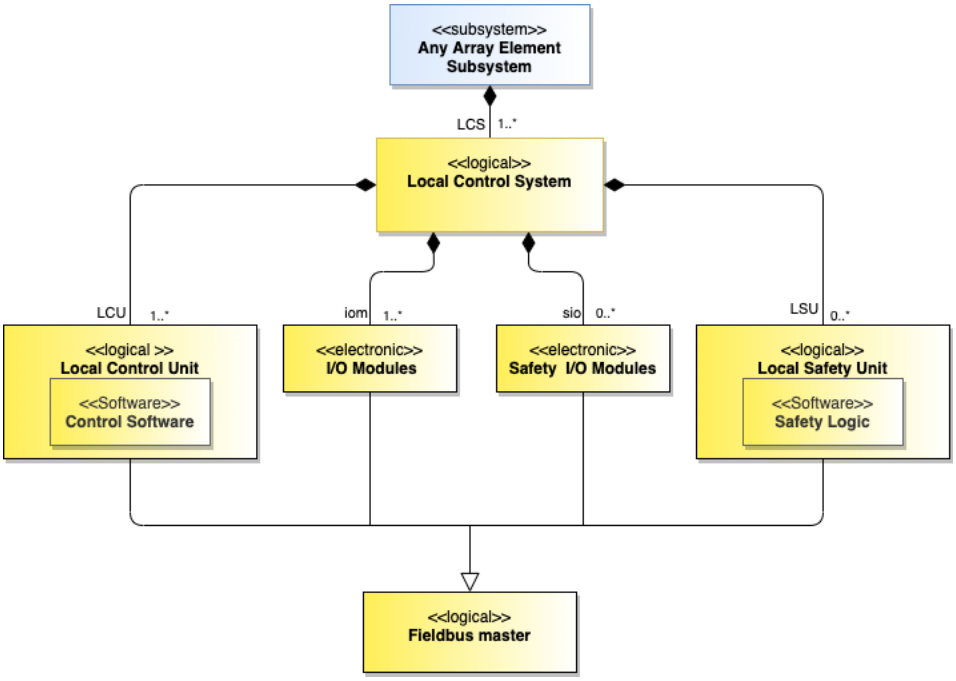

Figure 10- The generic architecture of an LCS

3.6.1 Control and Safety Units

An LCS is generally composed of two major sub-systems hereafter described.

- Local Control Unit: computing unit that monitors and assesses performance and health of the controlled system and manage fault detection and fault isolation functions.
- Local Safety Unit: computing unit responsible for all safety-related controls and monitoring system functions, as well as managing safety-related devices (interlocks) and the related logic chain.

In general, LCUs are PLCs or industrials PCs/ARM based computers, running real-time or standard operating system, other embedded systems like Field Programmable Gate Arrays (FPGAs)/micro-Controllers, etc. [RD-5].

The CTAO-X IPS supervises and interfaces to each Array Element through a safety communication layer and brings additional safeguards as may be required from CTAO-X/Array Element sub-system interactions, as they are integrated and will enter in operations. Commissioning and testing of an LCS shall be performed without dependency form external software system.

4 Definitions

The following terms and definitions are under review by different groups of the CTAO PO, and maybe different in further version of the document.

For every term, is indicated the standards or sources from where the definition has been adapted or taken. The definition of some terms are customized for the purpose of the project.

Actuator: Physical device for moving or controlling a mechanism or system. It is operated by a source of energy and converts that energy into motion. An actuator is a mechanism by which a control system acts upon an environment. The control system can be simple (a fixed mechanical or electronic system), software-based (e.g. a printer driver, robot control system), or a human or another agent. [NIST SP 800-82 Rev. 2]

Array Elements: A system deployed on an Array Site which is needed for the scientific operation of CTAO and which is interfaced to the ACADA and IPS systems. Array Elements (and in cases of sufficient complexity, such as that of a Cherenkov Telescope, also their sub-systems) are required to implement well-defined common Stathes. An Array Element consists of one or more Controllable Systems and may also include Sensors, plus a software system to manage these elements. [CTAO Glossary]

Array Element Manager: High-Level Software component, being installed at the data centre, that every Array Element interacting with ACADA should develop, responsible of receiving commands from ACADA and distributing them to the LCS components. [Customized]

Calibration Activities (Technical): All activities related to performing a comparison between a device under test and an established standard. It may also include adjustment of the instrument to align it with the standard [https://csrc.nist.gov/glossary/term/calibration].

Calibration Data: Updated and published data set providing information related to the non-scientific calibration purposes of the system. [Customized]

Command: Specific instruction given to a controllable item to perform/execute a specific kind of task or function. [Adapted from Oxford Languages dictionary]

Control System: Integrated hardware and software equipment that manages, commands, monitors and display the operation of a system, associated subsystems and devices (Systems under Control). Control system includes supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other type of control system such as Programmable Logic Controllers (PLC) and Remote Terminal Unit (RTU). [NIST SP 800-82 Rev. 2]

Control Unit(s): Computing unit(s) in charge of executing the control and monitoring functions related to the associated item (e.g. drive systems, conditioning system, etc). [Adapted from NIST SP 800-82 Rev. 2]

Controllable system: Any system on an Array Site to which can be applied the following two properties:

- Controllability, the ability of a system to reach a definite state from a fixed (initial) state in a finite interval of time. The transition can be triggered by an external input (command from another controller) or can be performed autonomously (Internal controller).
- Observability, which measures the ability of the configuration to supply all the information necessary to estimate all the states of the system. [Customized]

Controller: device or program that operates automatically to regulate a controlled variable. [IEC 61508-4-2020]

Display: The technology associated with an output device that presents information in visual form. [Oxford Languages dictionary]

Distributed Control System: An industrial control system in which the is control achieved by intelligence that is distributed about the process to be controlled, rather than by a centrally located single unit. DCS allows each section of a machine to have its own dedicated controller that runs the operation. A DCS has several local controllers located throughout the area that are connected by a high-speed communication network. [Adapted from NIST SP 800-82 Rev. 2]

Engineering HMI: HMI related to a particular system, able to provide to the user expert the capability to remotely operate that system for the engineering activities. [Customized]

Engineering Parameters: Category parameters of a system which are useful for the engineering activities on that system. [Customized]

Engineering Activities: All activities necessary to study the measurement and control of process variables, and the design and implementation of systems that incorporate them to guarantees an efficient functional behaviour of a system. [Adapted from "Industrial Instrumentation and Controls Technology Alliance"].

Engineering Data: Engineering test data, acquired as a result of engineering test, and used for further processing by the maintenance teams. [Customized]

Externally Controllable system: Control system designed to have the possibility to be controlled (command, monitoring, display) by a controller belonging to a different control system. [Customized]

Field Devices: Equipment that is connected to the field side on an Industrial Control System. Types of field devices include RTUs, PLCs, actuators, sensors, HMIs, and associated communications. [NIST SP 800-82 Rev. 2]

Field/Plant: The physical elements necessary to support the physical process. This can include many of the static components not controlled by the ICS. [IEC 61508-4-2020]

Fieldbus: A digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device. A protocol is used to define messages over the fieldbus network with each message identifying a particular sensor on the network. [IEC 61508-4-2020]

Finite State Machine: An abstract machine that can be in exactly one of a finite number of states at any given time. The FSM can change from one state to another in response to some external inputs; the change from one state to another is called a transition (State Transition). An FSM is defined by a

list of its states, its initial state, and the conditions for each transition. [http://foldoc.org/finite+state+machine]

Hardware Component: The material physical components of a system. [NIST SP 800-171 Rev.2]

Housekeeping Data: Set of information that must be available to serve the purposes of verification, maintenance, failure analysis, etc. but are not useful during operation. [Customized]

Human Machine Interface: The hardware or software through which an operator interacts with a controller. An HMI can range from a physical control panel with buttons and indicator lights to an industrial PC with a colour graphics display running dedicated HMI software. [NIST SP 800-82 Rev. 2]

Industrial Control System (ICS): An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. [Adapted from NIST SP 800-82 REV. 2]

Interlock: Mechanical, electrical, or another type of device, which purpose is to prevent the operation of hazardous machine functions under specified conditions. [ISO 14119:2013]

Internally Controllable system: Control system designed to receive control commands and display, by expert operators through its dedicated Engineering and Maintenance HMIs (the monitoring part can be covered externally). [Customized]

Local Access Mode: The ability of an authorized user or controller to operate the field-deployed controllable systems, communicating through a direct connection without the use of a network. Local Mode supports individual maintenance activities, and it is only available when the Machine State is set to OFF. In this state, all remote actions that could endanger the safety of a local person are prevented. Adapted from [NIST SP 800-171 Rev.2]

Local Control System: Control and safety units, control software, local communication infrastructure required to guarantee functional operation of a given equipment and all the other support elements needed for integration, verification and maintenance activities. [Customized]

Local Maintenance Access Mode: Local Access mode, where ACADA control part is detached, and the monitoring is active. The control of the instrument is performed through the Maintenance HMI on the field. The Machine State is set to MAINTENANCE. [Customized]

Long-Term Storage: System dedicated to the storage of information over an extended period (usually years). [Customized]

Machine State: A state that is intrinsic to the hardware state of an Array Element. These states and their transitions are not managed via the ACADA. The following Machine States exist: Off, On, Maintenance. [Customized]

Maintenance Activities: All activities necessary to keep an asset in, or restore it to a specified condition, keep it safe, reliable, and fit for service throughout the operational lifecycle phase. [CTAO Glossary]

Maintenance HMI: HMI related to a particular system, able to provide to the user expert the capability to locally operate that system for the maintenance activities. [Customized]

Maintenance Parameters: Category of a system parameters which are useful for maintenance activities on that system. [Customized]

Monitoring: The action of continual checking, supervising, critically observing, or determining the status of a system to identify change from the performance level required or expected. It includes detection and alerting about possible non-safety-related abnormal situations. [Adapted from NIST SP 800-160 Vol. 1]

Monitoring Data: Updated and published data set providing complete status information about the associated item equipment, function and performance. [Customized]

Non-safety related parameters: Category of system parameters that do not belong to Safety procedures, performance, and functions. [Customized]

Normal Operations Condition: Environmental conditions under which standard operation, engineering, maintenance, and Calibration activities may be undertaken, during day or night. [Customized]

Operational State: A logical state of the element with respect to the operations the element is performing. [Customized]

Parameter: Numerical or other measurable information related to an element of a system that is useful, or critical, when identifying the system, or when evaluating its performance, status, condition. [Oxford Languages dictionary]

Performance Level (PL): is a value used to define the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions. [ISO 13849-1]

Programmable Electronic System (PES): System for control, protection or monitoring dependent for its operation on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, contactors, and other output devices. [ISO 13849-1:2015]

Programmable Logic Controller (PLC): A solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing. Adapted from [NIST SP 800-82 REV. 2]

Remote Access Mode: The ability of an authorized user or controller to access computing resources to operate the system from a location other than the organization's facilities, communicating through an external network. The remote mode supports observatory science operation and system/array-level engineering activities. This access mode is only available when the Machine State is set to On. [Adapted from NIST SP 800-171 Rev.2]

Remote Array Access Mode: Remote Access Mode where ACADA has the full control of the instrument either for Maintenance, Technical or Scientific operations. The Machine State of the instrument is set to ON. No people are present on the field. [Customized]

Remote Engineering Access Mode: Remote Access Mode where ACADA control part is detached and the monitoring is active. The control is performed through the Engineering HMI. The Machine State of the Instrument is set to ON. No people are present on the field. This mode applies only

for the maintenance of a single instrument or 'not planned' engineering activities (e.g. Fault recovery, bug-fixing, problem-solving). [Customized]

Safe State: The state of the process after acting to remove the hazard resulting in no significant harm. [IEC 61508, functional safety]

Safety Function: is a safety- related control function of a machine that reduces the risk presented by the machine to an acceptable level. [EN ISO 13849-1 ,Safety Related part of Control Systems]

Safety Integrity Level: Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest. [ISO/IEC/IEEE 24748-4:2016]

Safety operations: All activities, procedure and operations performed by the system which include the execution of safety functions as defined in ISO 13849-1:2015. [Customized]

Safety related parameters: Category parameters of a system that belong to the Safety procedures, performance, and functions as defined in ISO 14119:2013. [Customized]

Safety Unit(s): Computing nodes in charge of executing the safety-related functions of the associated item. [Customized]

SCADA: Supervisory Control and Data Acquisition (SCADA) is an industrial control system that provides the high-level centralized control, monitoring and display of a wide variety of peripheral devices such as Programmable Logical Controller (PLC) or Remote Terminal Units (RTU)'. Adapted from [NIST SP 800-82 REV. 2]

Science Data: Information collected with the Array Elements, or processed with the CTAO software systems, for a specific purpose of studying or analysing scientific phenomena with CTAO. [Customized]

Sensors: A device that produces a voltage or current output that is representative of some physical property being measured. [NIST SP 800-82 REV. 2]

Short-Term Storage: A system dedicated to the real-time acquisition and temporary storage of information (from days to several weeks). [Customized]

Software Component: A software package, service, resource, or module that encapsulates a set of related functions or data. A software component can be deployed independently and is subject to composition by third parties. [Customized]

State: The condition of a system, subsystem, etc., resulting from a combination of functions being activated and structured according to a specified scheme or strategy, usually under supervision by a control system. [Customized]

Storage: The retention of retrievable data on a computer or other electronic system. [Oxford Languages dictionary]

Sub-state: A state within another state, where transitions can be managed and triggered internally by the system according to external conditions (e.g. available time inside the current state). [Customized]

Supervisor: Group of SW and HW equipment inside the instrument dedicated to the coordination of the field devices and the management of the safety (e.g. PLCs, Safety PLC). The Supervisors can be deployed at the array element or in the data center. [Customized]

Technical Operations: The subset of normal operations that include engineering, maintenance, and calibration activities for non-scientific purposes. [Customized]

Technical Data: Updated and published data set providing information related to the engineering and maintenance purposes of the system. [Customized]