Programme: ELT

Project/WP: Telescope Control

Control System Development Standards

Document Number: ESO-193358

Document Version: 9

Document Type: Specification (SPE)

Released On: 2022-08-04

Document Classification: ESO Internal Use [Confidential for Non-ESO Staff]

Owner:	Kornweibel, Nick
Validated by PM:	Kornweibel, Nick
Validated by SE:	González Herrera, Juan Carlos
Validated by PE:	Biancat Marchet, Fabio
Approved by PGM:	Tamai, Roberto

Name

Released by ESO PDM SYSTEM

Authors

Name	Affiliation
N. Kornweibel	ESO

Change Record from previous Version

Affected Section(s)	Changes / Reason / Remarks
	See CRE ET-1266
AD03	version updated (coding standards) ESO-254539/5 (See CRE ET-1215)
AD04	updated (ICD to NI) ESO-320983/3 (See CRE ET-1124)
AD05	update (ICD to TRS) ESO-331947/2 (See CRE ET-1085)
AD06	added to replace internally maintained list in Req 398 (ESO List of PLC modules)
AD07	added (List of Ethernet Cards for Servers)
RD33	updated (external to XML reference obsolete/replaced)
RD44	updated MUDPI standard
RD45	ZPB standard version update
RD55	ELT PBS version updated
Req 1	added DDS as middleware standard (this was an omission, was always a middleware standard and was listed elsewhere, just not here)
Req 155 (info)	expanded to include ICS (instrument control systems)
Section 5.1	removed various network requirements already covered in ADs (Req 365, 366, 425, 3, 4, 5, 6, 7, 8, 9, 13, 14, 15, 16, 432).
Req 5, 15	removed
Req 431	clarified which specific network types AD4 was applicable too.
Req 439	Added; The list of supported Ethernet cards is given in AD07.
Req 440	Added; The requirements for the interfaces between the control network and its clients are specified in AD04 and AD05. This applies to the entire control network including local control networks.

Req 441	Added; Specifying interface requirements to TRS according to AD05.
Req 371 (info)	Expanded info on the use of NTP.
Req 20, 31 and 374	removed Matlab as a standard.
Req 83	clarification added.
Req 394, 424	various software package versions updated. Matlab removed. Nix removed.
Req 398	List of PLC modules removed from this document and text replaced to reference to AD6.
	Misc. typos/spelling corrections

Contents

[R-CSD-110] / / /

Abbreviations and acronyms

[R-CSD-111] / / /

The following table collects those used throughout this document.

CCS	Central Control System
CI	Configuration Item
DDS	Data Distribution Service
FBD	Function Block Diagram
FPGA	Field Programmable Gate Array
LCS	Local Control System
ICS	Instrument Control System
OLE	Object Linking and Embedding
OPC	OLE for Process Control
OPC UA	OPC Unified Architecture
PLC	Programmable Logic Controller
PTP	Precision Time Protocol
ST	Structured Text
VHDL	Very High Speed Integrated Circuit Hardware Description Language

1. Scope

[R-CSD-114] / / /

This document specifies the development standards applicable to any control system part of the telescope or its subsystems, including Local Control Systems and Instrument Control Systems. That is, it specifies the standards to be employed when developing any hardware, software and communication infrastructure required to control the telescope down to, but not including, actuators and sensors.

[R-CSD-338] / / /

It applies to both ESO internal and external parties developing parts of the control system of the ELT.

[R-CSD-115] / / /

The requirements for the Central Control System are still in preparation, and may result in additions to the set of supported runtime and development platforms and programming languages.

2. Related documents

2.1 Applicable documents

[R-CSD-118] / / /

The following applicable documents form a part of the present document to the extent specified herein. In the event of conflict between applicable documents and the content of the present document, the content of the present document shall be taken as superseding.

2.1.1 General

2.1.2 Programming languages

AD01 VHDL language reference manual;
IEEE Std 1076-2000

AD02 Programmable controllers – Programming languages;
IEC 61131-3:2013

AD03 ELT Programming Language Coding Standards;
ESO-254539 Version 5
https://pdm.eso.org/kronodoc/HQ/ESO-254539/5

AD04 ICD between the Network Equipment and its Clients;
ESO-320983 Version 3
https://pdm.eso.org/kronodoc/HQ/ESO-320983/3

AD05 ICD between ELT TRS and the TRS Clients;
ESO-331947 Version 2
https://pdm.eso.org/kronodoc/HQ/ESO-331947/2

AD06 List of PLC Modules
ESO-253356 Version 4
https://pdm.eso.org/kronodoc/HQ/ESO-253356/4

AD07 Standard Ethernet Cards for ELT Control System Servers
ESO-385223 Version 3
https://pdm.eso.org/kronodoc/HQ/ESO-385223/3

2.2 Reference documents

2.2.1 General

RD01 ESO Safety Conformity Assessment Procedure;
SAF-GEN-MAN-3444 Version 5
https://pdm.eso.org/kronodoc/HQ/ESO-193497/5

RD02 Obsolescence management – Application guide;
IEC 62402:2007

2.2.2 Communication

RD21 Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 3;
IEEE Std 802.3-2009

RD22 Industrial communication networks - Fieldbus specifications - Type 10 elements (PROFINET);
IEC 61158-6-10:2007

RD23 Industrial communication networks - Profiles - Functional safety fieldbuses;
IEC 61784-3-3:2007

2.2.3 Notational standards

RD31 Quantities and units;
ISO 80000

RD32 Data elements and interchange formats - Information interchange – Representation of dates and times;
ISO 8601:2004(E)

RD33 Information technology - Document description and processing languages - Office open XML file formats;
ISO/IEC 29500-1:2016

2.2.4 Services

RD41 Precision clock synchronization protocol for networked measurement and control systems;
IEEE Std 1588-2008

RD42 Network time protocol;
RFC 1305, Version 3

RD43 OPC Unified Architecture Specification;
IEC 62541

RD44 MUDPI Format;
ESO-302020 Version 5
https://pdm.eso.org/kronodoc/HQ/ESO-302020/5

RD45 Data Transport Format for ZeroMQ;
ESO-321056 Version 2
https://pdm.eso.org/kronodoc/HQ/ESO-321056/2

RD46 Data Distribution Service Interoperability Protocol;
https://www.omg.org/spec/DDSI-RTPS/About-DDSI-RTPS/

2.2.5 Other

RD55 ELT Product Breakdown Structure;
ESO-232484 Version 9
https://pdm.eso.org/kronodoc/HQ/ESO-232484/9

3. Introduction

[R-CSD-155] / / / The document defines the development standards for the ELT Central Control System (CCS) and all its components as well all Local Control Systems (LCS) and Instrument Control Systems (ICS) of the ELT.

For ease of reading, the term CS (for Control System) shall refer to both the Control System component of the ELT (product 449 in [RD55]) as well all Local Control System components of the ELT (for example products 241, M1 Local Control System, 366 M2 Local Control System, 428 Dome Local Control System, and so on, per [RD55]).

[R-CSD-156] / / / The development standards define the elements of the hardware and software infrastructure, development process and product assurance requirements that shall be strictly applied throughout the CS to ensure a consistent level of quality and enable seamless integration of subsystems.

[R-CSD-157] / / / The development standards present manufacturers and developers with a (small) variety of solutions to design and implement their component(s) of the CS. For example, Local Control Units (LCU) may be implemented on either Programmable Logic Controller (PLC), embedded computers running real-time or standard Operating System (OS), etc.

[R-CSD-158] / / / For the Interlock and Safety System (ILS) and the implementation of the safety-related functions pertaining to the Local Control System (LCS), a single platform is enforced.

[R-CSD-159] / / / Well-established industrial standards and Commercial Off-The-Shelf (COTS) products are promoted and custom-built solutions are strongly discouraged.

[R-CSD-161] / / / The versions of standards or products referenced in this document are subject to a periodic update as the ELT projects progresses.

[R-CSD-163] / / / Note: The term contractor applies to the control system development team regardless of its affiliation (i.e. ESO or third-party).

4. Infrastructure Standards

[R-CSD-1] D/ /I/ For inter or intra component communication the following communication technologies shall be used:

- Ethernet, according to RD21.
- PROFINET IO with PROFIsafe, according to RD22 and RD23 respectively.
- Unicast and Multicast UDP/IP.
- MUDPI, according to RD44.
- ZeroMQ/Protobuf according to RD45.
- OPC Unified Architecture (OPC UA), according to RD43.
- Data Distribution Services (DDS), according to RD46

[R-CSD-2] D/ / / The use of an alternative standard for a particular purpose shall be declared, justified and is subject to approval by ESO.

5. Interface Standards

[R-CSD-168] / / / The communication infrastructure establishes four communication channels:

- Control network,
- Deterministic network,
- Interlock and safety network,
- Time reference network.

[R-CSD-169] / / / This section specifies the interfaces to these four communication channels common to all telescope subsystems, i.e. physical interfaces and protocols. It is understood that command and data format, rates, QoS, etc. are specific for each subsystem and therefore defined in each subsystem ICD.

5.1 General

[R-CSD-431] D/ / / Network nodes on Control, Deterministic and Time Reference networks shall comply with the interface standards and network services according to AD04.

[R-CSD-439] D/ / / The list of supported Ethernet cards is given in AD07.

[R-CSD-440] D/ / / The requirements for the interfaces between the control network and its clients are specified in AD04 and AD05. This applies to the entire control network including local control networks.

5.2 Control network

[R-CSD-368] / / / The control network provides infrastructure for the transmission of control and monitoring data between control and computing units in the CS. Each CS component will be associated to an ICD to document the data interface to the control network.

5.3 Deterministic network

[R-CSD-369] D/ /I/ The Deterministic network provides distributed control applications with a communication media of predictable latency and response time. Guaranteeing the required latency and determinism over Ethernet implies that bandwidth saturation or bursts of near maximum

network load must be prohibited. For this reason, access and use of the Deterministic network is limited. If a CS component requires access to the deterministic network, it will be specified in the associated ICD for that component.

5.4 Interlock and safety network

[R-CSD-370] / / / The interlock and safety network is provided for, and dedicated to, the integration of CS component safety units with the telescope interlock and safety system.

5.4.1 Physical layer

[R-CSD-10] D/ /I/ 100BASE-TX shall be used, according to RD21.

5.4.2 Data link layer

[R-CSD-11] D/ /I/ Ethernet shall be used, according to RD21.

5.4.3 Application layer

[R-CSD-12] D/ /I/T PROFINET IO with PROFIsafe according to RD22 and RD23 respectively.

5.5 Time reference network

[R-CSD-371] / / / The time reference network is dedicated to the transport of protocols for synchronizing the clocks of control and safety units in the CS.

It is worthwhile noting that NTP is transported over the control network and therefore doesn't require a dedicated physical network adapter interface, but PTP is transported over a dedicated PTP time reference network and requires a dedicated physical network adapter interface on a connected client.

[R-CSD-441] D/ / / Interfaces to the Time reference network shall follow AD05.

6. Notational Standards

6.1 Quantities and units

[R-CSD-17] D/ /I/ Quantities and units shall follow the International System of Quantities and International System of Units, according to RD31.

[R-CSD-18] D/ /I/ The time stamps exchanged in data communication protocols shall be expressed in TAI time standard with epoch set to 1 January 1970 00:00:00 TAI, which is 31 December 1969 23:59:51.999918 UTC.

[R-CSD-19] D/ /I/ The time representation format (i.e. as presented in GUI, reports, etc., for "human consumption") is yyyy-mm-ddThh:mm:ss.ff according to RD32 and expressed in UTC timescale. The resolution shall be as needed by the application, i.e. the fractional seconds are optional and could go down to nanosecond resolution.

Note that the integral portion of the seconds field for a timestamp during a leap second insertion is formatted as "60".

6.2 Programming languages

6.2.1 Local control system

6.2.1.1 Local control units

[R-CSD-20] D/ /I/ The code delivered for each language shall be compliant with one of the following:

- VHDL according to AD01.
- Function Block Diagram (FBD) and Structured Text (ST) according to AD02.
- C++, (coding standards per AD03).
- Java Standard Edition (SE), (coding standards per AD03).
- Python, (coding standards per AD03).
- LabVIEW G, (coding standards per AD03).

[R-CSD-21] D/ /I/ Usage of C programming language shall be restricted to source code for building libraries and software components for embedding and linking in other software. This includes the use of C++ when employed in a purely procedural manner.

Language bindings to libraries of different languages shall be done via the C language (e.g. Java binding to a C++ library shall do so via a C interface and not directly to C++).

6.2.1.2 Local safety units

[R-CSD-23] D/ /I/ FBD (limited to failsafe instruction set) shall be used.

6.2.1.3 Graphical user interfaces

[R-CSD-374] D/ /I/ The following programming languages/platforms are available for the development of engineering, maintenance and test GUIs for control as well as local safety units:

- Visual C++ (Windows forms with C++/CLI).
- LabVIEW G (for larger or complex GUI, this is discouraged).
- Touch panel HMI (limited to simplistic interfaces on PLC-based systems).
- Java SE.
- Python.
- Qt.

[R-CSD-376] D/ /I/ Communication between GUI and the LCU and LSU is subject to the same infrastructure and interface standards as defined in this document.

7. Implementation

7.1 Runtime platforms

[R-CSD-24] D/ / /
The use of an alternative runtime platform standard for a particular purpose shall be declared, justified and subject to approval by ESO.

7.1.1 Local control system

7.1.1.1 Local control units

[R-CSD-25] D/ /I/
The runtime platform shall be one of the following:

- SIMATIC S7,
- TwinCAT,
- LabVIEW RT.
- Linux and LinuxRT (per 10.1)

7.1.1.2 Local safety units

[R-CSD-28] D/ /I/
The runtime platform shall be exclusively Failsafe SIMATIC S7 for all telescope systems.

[R-CSD-427] D/ /I/
The runtime platform shall be Failsafe SIMATIC S7 or Beckhoff TwinSAFE for instrument control systems.

7.2 Development environments

[R-CSD-29] D/ /I/
The development platform shall be Microsoft Windows.

All source code shall be developed in the English language, using development tools in the English language.

[R-CSD-30] D/ / / The use of an alternative development platform standard for a particular purpose shall be declared, justified and subject to approval by ESO if it is required to build, test, maintain or operate the delivered system.

7.2.1 Local control system

7.2.1.1 Local control units

[R-CSD-31] D/ /I/ The software development environment for control unit software shall be comprised of and limited to:

- LabVIEW IDE,
- MS Visual Studio IDE, restricted to C/C++ programming languages (and TwinCAT),
- Eclipse IDE, restricted to C++ (Linux only), Java and Python,
- Siemens TIA Portal,
- Beckhoff TwinCAT,
- Git client.

7.2.1.2 Local safety units

[R-CSD-32] D/ /I/ The software development environment for safety unit software shall include:

- SIMATIC Safety Advanced.
- TwinSAFE.

8. Tools

8.1 Control engineering

[R-CSD-33] D/ /I/ The analysis of control systems (e.g. for performance assessment analysis and to support the definition of control algorithms) shall be performed with widely adopted, well recognized software packages, subject to ESO approval. MATLAB/Simulink are the preferred software packages to perform servo control loop simulations.

[R-CSD-417] D/ /I/ All the models used to verify compliance of the controlled system against control requirements shall be a deliverable to ESO.

[R-CSD-380] D/ /I/ Control algorithms developed with a numerical computing environment, which are to be integrated into control applications, must be done so using available cross-language support tools (e.g. mathscript nodes in LabVIEW).

8.2 Version control

[R-CSD-34] D/ / / The contractor shall use a version control tool.

[R-CSD-35] D/ /I/ The contractor shall deliver to ESO version control system repository (Git) to a URL provided by ESO.

9. Product Assurance

9.1 Quality assurance

[R-CSD-381] / / /
The following sections include a set of requirements specifying:

- Analyses, inspections and tests to be performed throughout the development process,
- Properties of the development process,
- Content and quality of control system relevant documentation.

That are deemed necessary to ensure compliance with ESO's quality standards.

9.1.1 Analysis requirements

[R-CSD-36] D/A/ /
The characteristics of the components of the control system shall be derived from hazard, reliability, risk and control analyses.

[R-CSD-38] D/ /I/
The control objective of control problems shall be formulated in a quantitative and verifiable form. The performance requirements shall be derived from the relevant top-level requirements.

[R-CSD-39] D/ /I/
Control analysis shall be performed by breaking down the control and plant critical functionalities into functional units modelled as linear systems (static and dynamic); in case any linearization is performed, the relevant working regime shall be identified.

[R-CSD-40] D/ /I/T
The performance of the controlled system shall be evaluated taking into account the relevant external and internal perturbations and the expected/measured behaviour of its components (including but not limited to friction and backlash in mechanical components, effect of sampling and quantization, delays introduced by computing units and non-linear behaviour of sensors).

[R-CSD-41] D/A/ /T
A strategy to assess the robust performance of the controlled system over the entire operational range shall be defined and applied.

[R-CSD-42] D/A/ /T
A strategy to assess the robust stability of the controlled system over the entire functional range shall be defined and applied.

[R-CSD-418] / / /
The use of decentralized controllers for Multiple-Inputs-Multiple-Outputs (MIMO) plants is preferred.

[R-CSD-419] / / / Controller design that is linear, Single-Input-Single-Output (SISO) and time invariant are preferred.

[R-CSD-382] /A/ /T If not stated differently in the corresponding subsystem specification, the controlled system shall satisfy the MIMO stability margin ||S(jw)||∞<2, being S(jw) the frequency-dependent sensitivity function of the closed-loop system.

Note: In case of SISO system the above mentioned requirement amounts to ensure at least 6dB modulus margin which in turn implies the standard rules of Gain Margin larger than 6dB and Phase Margin larger than 30 degrees.

9.1.2 Inspection requirements

[R-CSD-45] D/ /I/ The code delivered for each programming language shall be periodically inspected by ESO (or an ESO representative), static and dynamic properties (for example dependency, complexity, memory corruption, coverage) evaluated against acceptance criteria and results communicated to the supplier for remedial action.

[R-CSD-384] D/ /I/ The contractor shall upload the latest stable software source code to ESO's version control system repository at least once per quarter year.

9.1.3 Test requirements

[R-CSD-47] / / /T The performance of the controlled system in the operational range shall be assessed by test. This includes the measurement of the closed loop frequency responses, test of the robustness of stability and of the system response to excitation signals such as step, impulses, sine waves and user-defined signals.

[R-CSD-420] / / /T Correct performance and function of the system shall be verifiable at subsystem and subsystem component level through the execution of automatic tests.

[R-CSD-48] D/ /I/ A test infrastructure for automatic tests and static and dynamic analysis of subsystem components shall be used and approved by ESO.

[R-CSD-49] D/ / /T For every data interface provided and requested by the control system, it shall be possible for the provider and requester to test its behaviour (functionality and performance) in the absence of the other (that is, it shall be possible verify interfaces via use of simulation modes).

[R-CSD-50] D/ /I/T Every release (after final design review) shall be accompanied by integration and system test suites.

[R-CSD-51] D/ /I/ A strategy to allow for measurement of the frequency response of the controlled system both in closed and open loop shall be defined. This shall include the identification of parametric models for control design.

[R-CSD-385] D/ /I/ A strategy to allow for injection of excitation signals at servo loop frequency, and probing of signals at servo loop frequency (at least including controller output and measurements

of plant's output) shall be defined. It shall be possible for the user to configure the characteristics of the excitation signals (type of signal, e.g. step, sine wave, impulse, signal amplitude and sampling rate) in order to span both the controlled system's functional and operational range.

[R-CSD-410] D/ /I/ To support post-mortem examination of performance, it shall be possible to retrieve a time series recording (recorded at controller servo loop frequency) of controlled and commanded variables for a period of time appropriate to identify instability and performance degradation events (for example five seconds of closed loop control data would be seen as suitable for a 500Hz loop).

9.1.4 Development process requirements

[R-CSD-52] D/ / / The development process shall be appropriate to the size and complexity of the project. The process shall be documented in the Control system project management plan.

[R-CSD-53] D/ / / A defined incremental and iterative development process with defined activities, phases, deliverables and milestones, approved by ESO, shall be used by the control system contractor.

[R-CSD-54] D/ / / The development process shall at least foresee the delivery of the following documents pertaining to the control system:

- Control system project management plan,
- Control system analysis report(s),
- Control system design description,
- Control system test documentation,
- Control system transfer document,
- User manual(s).

Note: For practical reasons and if the size and the complexity of the project allows it, each one of the documents mentioned in the following sections could be integrated into a higher-level document.

[R-CSD-56] D/ / / After first delivery, an up-to-date version of the deliverable has to be provided at every following milestone. The delta with respect to the previous milestone has to be reviewed.

9.1.5 Documentation requirements

9.1.5.1 General

[R-CSD-57] / /I/ The documentation produced shall be in English language.

[R-CSD-58] D/ /I/ All documents shall be available in electronic format, according to RD33.

[R-CSD-59] D/ / / All documents shall be under version control.

[R-CSD-60] D/ /I/ For every item (including 3rd party and COTS components) the original documentation shall be delivered, in English if available.

9.1.5.2 Control system project management plan

[R-CSD-61] D/ / / This document shall address the project organization, processes, tasks, milestones and deliverables, schedule, and resource, QA and configuration management plan.

9.1.5.3 Control system analysis reports

[R-CSD-65] / /I/ The documents shall describe the methods and results of the hazard, reliability, risk, control and performance analyses carried out throughout the control system development phase.

[R-CSD-66] / /I/ The hazard analysis report shall describe the method and results of the hazard analysis.

[R-CSD-67] / /I/ Reliability and failure modes of components of the control system yielding a hazardous situation in terms of human health or equipment integrity shall be addressed and documented as part of the hazard analysis report.

[R-CSD-68] / /I/ Reliability and failure modes of the components of the control system impacting availability or maintainability of the system shall be analyzed and documented in a reliability analysis report.

[R-CSD-69] / /I/ The reliability analysis report shall identify the means to detect and isolate each identified component failure. For example: visual inspection, automatic test, on-line signal or metric monitoring.

[R-CSD-70] / /I/ The risk analysis report shall describe the risks pertaining to the development and operation of the control system, being that of organizational, architectural or technical nature, and appropriate mitigation strategies.

[R-CSD-71] D/ /I/ Obsolescence risks shall be described and appropriate obsolescence management strategy for both software and hardware components allowing purchasing the necessary parts or services in a competitive environment shall be documented. For background and further reference, please see RD02.

[R-CSD-390] / /I/ The control analysis report shall describe methodology and results of all the analyses performed in order to support the selection of the control architecture and components, i.e. shall focus on breaking down the control-relevant performance-critical requirements in terms of lower-level requirements for each component of the control system.

[R-CSD-72] / /I/ The control analysis report shall contain:

- The problem statement with a quantitative description of the control objective.
- A description of the plant model used for control design. Such a description shall include either a state space or a transfer function representation of the controlled plant.
- A control block diagram showing the relevant control system context. This shall include the dynamic response of the plant, the controller and the relevant inputs and outputs (including disturbances). A physical type shall be assigned to all signal flows.
- A description of the applied controller synthesis method demonstrated in a Bode or Nyquist diagram.
- The controller transfer functions (gain-pole-zero and/or state-space representation) and parameters.
- If applicable, any additional logic (e.g. anti-reset-windup protection) described in block-diagram form, pseudo-code or mathematical formulation.
- The derived closed loop transfer functions.
- The time response of the controlled system to step, impulse, sine-wave and general user-defined excitation signals injected at all the relevant interfaces of the closed loop system. The amplitude of the input signals shall be selected in order to cover both operational and functional range.
- The performance obtained using simulation or analytical calculations in order to demonstrate compliance of the controlled system to the control relevant requirements.
- The timing requirements relevant for the selected design in terms of sampling period, latency and jitter.
- The sensitivity analysis necessary to select possible hardware components (in terms of e.g. sensor noise or resolution of output) and their mutual location in the system (e.g. co-location properties).
- The results of the analysis aiming at assessing robustness of stability and performance of the controlled system.

[R-CSD-73] / /I/ The software analysis report shall describe the methodology and results of the analysis in terms of software and provide the necessary input to the software design. In particular the software analysis report shall contain:

- An overview of the software structure.
- The identification of critical software components.
- An assessment of the relative risk areas within the software system.
- An assessment of test coverage and tests to be developed.

9.1.5.4 Control system design description

[R-CSD-74] / /I/ The control system design description shall at least contain a description of the design constraints, decisions, static structure and dynamic behaviour, interfaces and data model of the control system.

[R-CSD-75] / /I/ The control system design description shall contain a description of all the specified top-level and lower-level components of the control system.

[R-CSD-76] / /I/ In particular, for every 3rd party or COTS product part of the control system, a reference to the relevant product description documentation describing main characteristics, measured/estimated performance and required interface shall be included in the document.

[R-CSD-77] / /I/ The control system design description shall contain a detailed description of all control system internal interfaces in particular including all relevant scaling factors, coordinate transforms, delays and timing constraints.

[R-CSD-386] / /I/ The control system design description shall detail how the control relevant requirements and the results of the analyses specified in Section 9.1.1 are reflected in the control system design.

[R-CSD-387] / /I/ In particular, the control system design description shall also contain traceability matrices from the components of the control system design to the requirements specification and conclusions of the analysis reports.

[R-CSD-388] / /I/ The control system design report shall contain the software architecture (with reference design patterns), static structure, dynamic behavior, deployment model and interfaces.

9.1.5.5 Control system test documentation

[R-CSD-78] / /I/ Separate test documentation shall be provided for functional, performance, integration and acceptance tests.

[R-CSD-79] / /I/ The documents shall describe the test plan, design, infrastructure and procedures.

[R-CSD-80] / /I/ For each test procedure, preconditions, assessment method (e.g. data processing algorithm), level of criticality and expected results shall be described.

[R-CSD-81] / /I/ The test documentation shall contain a traceability matrix in form of a table where requirement identifier, requirement short description, and reference to the test procedure are provided.

[R-CSD-82] / /I/ Separate test reports shall be produced for each individual execution of the test procedures.

[R-CSD-389] / /I/ In particular, the test report shall describe the final setup used in the tests and, if applicable, details on where this differs from the one defined in the verification plan.

9.1.5.6 Control system transfer document

[R-CSD-83] / /I/ This document shall describe installation procedures, build procedures, configuration item list, a summary of the acceptance test report, and the list of problem reports, change requests and non-conformance reports pertaining to the control system.

Regarding all 3rd party software products (including purchased and public domain), the Control System Transfer Document shall include:

- A list of all 3rd party software products, including version number and expansion modules, required to build and operate the control system.
- A statement that all control system software delivered to ESO is free from any restrictions arising from, for example, third party rights or other licensing conditions that could limit any of ESO's rights, except if expressly accepted by ESO in writing.

9.1.5.7 Control system user manual

[R-CSD-84] / /I/ This document states what the control system does, how it is operated and maintained.

[R-CSD-85] / /I/ There shall be a dedicated section for every 3rd party or COTS product which:

- Describes function and usage,
- Provides the necessary configuration,
- Identifies its version,
- Documents procedures for upgrades and updates.

9.2 RAMS requirements

9.2.1 Reliability

[R-CSD-306] / /I/ Testing coverage shall reflect appropriate focus on identified risk areas, determined through system analysis and documented as part of the Control System Analysis Reports.

9.2.2 Availability

[R-CSD-308] D/ /I/T Error handling shall enable identification of failure source and events.

[R-CSD-351] D/ /I/T Failure propagation and error handling shall be isolated to the affected component and not prevent continued use of the control system for functions unrelated to the failure. That

is, physically decoupled or functionally separate components shall not become coupled through the control system.

9.2.3 Maintainability

[R-CSD-86] D/ /I/ COTS components shall be used, subject to approval by ESO.

[R-CSD-87] D/ / / Bespoke hardware developments shall be avoided.

[R-CSD-88] / /I/ Auxiliary tools required to build, deploy, use, calibrate and test the control system shall be part of the control system deliverables.

[R-CSD-342] D/A/I/T The same development standards shall apply to all deliverables, including test, integration, verification and calibration components.

[R-CSD-343] D/ /I/T Control system hardware components must be accessible for dismounting and replacement in-situ in less than 30 minutes by a single individual, without the use of any special access tools.

[R-CSD-344] D/ / /T Software deployment to control and safety units shall complete in less than 3 minutes.

[R-CSD-345] D/ / /T There shall be no need for physical proximity or local intervention to the control and safety units, in particular during routine observations. All status and controls, as well as reset/restart/power cycling functions, remote flashing and software upload shall be under software control and accessible remotely.

[R-CSD-346] D/ /I/ Control system components shall be accessible for inspection without the use of any special tools and be possible with the control system in operation.

[R-CSD-347] / /I/ The code delivered for each language shall be compliant with the coding standards defined in AD01 through to AD03.

[R-CSD-348] / / / ESO will maintain and make available a registry of versions of tools, compilers and development environments for use with the supported programming languages for control units.

[R-CSD-349] / / / ESO will maintain and make available a registry of versions of tools, compilers and development environments for use with the supported programming languages for local safety units.

9.2.4 Maintenance approach

[R-CSD-339] D/ /I/ COTS components shall be used for their intended purposes.

[R-CSD-340] D/ /I/ Use of interface and abstraction shall be promoted to decouple components in the control system and promote ease of replacement of components of equivalent function and specification.

[R-CSD-341] D/ /I/ The control system shall not rely on function or performance available only in a specific version of COTS components which are not deemed forwardly compatible. That is,

components should be employed for their intended purpose and side effects or defects of a product or particular version of a product should not be leveraged.

9.2.5 Safety

[R-CSD-89] D/ /I/ The risk score of any control system hazard shall follow the ESO risk acceptability approach (see section 8.3 of RD01).

[R-CSD-90] / /I/T Following the risk assessment, alarms shall be raised and/or interlocks shall be implemented by the control system when approaching safety or performance critical conditions.

9.3 Strategic reuse requirements

[R-CSD-91] / /I/ Used or developed hardware components, software libraries, design patterns shall be systematically declared, documented, their functionality identified and justified.

[R-CSD-92] D/ /I/ Whenever applicable, control system components shall be chosen from the list of ESO approved standard components, defined in section 10.

9.4 Configuration management requirements

[R-CSD-93] D/ / / A change and defect management system shall be used, approved by ESO.

[R-CSD-95] / /I/ All Configuration Items (CI) (including but not limited to hardware components, software modules, documents, third party products) that are needed, used, produced by the system development and testing and/or needed for the operation are subject to configuration control. As such, shall:

- Have a (project) unique identifier,
- Be stored in a controlled place from which can be retrieved,
- Be subject to Change Management.

[R-CSD-96] / /I/ Every workable combination of hardware and software (baselines) shall clearly identify the components (ID, version) that they use. The baseline definition is also subject to Configuration Control.

[R-CSD-97] / /I/ Every identifiable deliverable shall be under configuration control, e.g. documents, developed source code. This includes source code, PLC source code and configuration, FPGA source code, external libraries, configuration data, operating system releases or patches, development environment, hardware serial numbers and hardware configuration.

[R-CSD-98] / /I/ Test data shall also be maintained under version control and tied to the specific release.

[R-CSD-99] / /I/ Third party code shall be under separate revision control and clearly identified as such.

[R-CSD-100] / /I/ A procedure to verify the operational system/components version shall be provided.

[R-CSD-101] / /I/ A procedure to verify the operational system configuration shall be provided.

[R-CSD-102] / /I/ A procedure to modify the operational system configuration (for example, component version, application or OS patch) shall be provided.

[R-CSD-421] / /I/ The software shall include a build script (or tool).

[R-CSD-422] / /I/T The software built script shall automatically (programmitcally) retrieve source code from the version control system, build and deployed the software.

[R-CSD-103] / /I/ The software build script shall identify source code dependencies between packages.

[R-CSD-104] / / /T The software build shall be incremental and repeatable.

[R-CSD-105] / / /T The deployment of a control system shall start from the lowest configuration level possible and work upwards, providing a means to verify the system at increasing levels of integration.

10. Equipment and Component List

[R-CSD-106] / / / ESO will maintain a register of accepted, standard, hardware and software products for use in construction of control systems.

[R-CSD-107] / / / The register will be updated and reissued approximately annually.

The final control system delivery must reflect the hardware and software products of the latest issue of the register, at the time of delivery.

10.1 Register of Accepted Standard Software Products

[R-CSD-394] D/ / / All software products listed are the English language version.

Windows platform:

Microsoft Toolkit	Release	64/32 bits
Operating System	Windows 10 Enterprise	64
Visual Studio	2017	--
Plugin Silverlight for IE	5.1.20125.0 or higher	64
LabVIEW Toolkit	**Release**	
LabVIEW	2021	32
LabVIEW RealTime	2021	32
LabVIEW FPGA	2021	32
LabVIEW Xilinx	2020	32
Beckhof Toolkit	**Release**	
TwinCAT3	3.1.4024.7	64
Siemens Toolkit	**Release**	
SIMATIC STEP 7 Prof. (TIA)	Latest commercial version and update	64
SIMATIC STEP 7 Safety Advanced (TIA)	Latest commercial version and update	64
SIMATIC WinCC Comfort (TIA)	Latest commercial version and update	64
SINAMICS Starter	Latest commercial version and update	64

SINAMICS DCC Combo (Drive Control Chart)	Latest commercial version and update	64
SINAMICS Startdrive Advanced	Latest commercial version and update	64
Drive ES	Latest commercial version and update	64
SIMATIC OPC UA S7-1500 (Small, Medium and Large)	Latest commercial version and update	
Other Software	**Release**	
OPC UA Client – UaExpert	1.4.4 or higher	32
Filezilla	3.27.0.1 or higher	64
SVN Tortoise	1.9 or higher	64
Wireshark	2.4.0 or higher	64
Adobe PDF Reader	18.011.20038 or higher	64
PuTTY	0.70 or higher	64
Eclipse SDK	4.7.0 Oxygen or higher	64

[R-CSD-424] D/ / /

All software products listed are the English language version.

Linux Platform:

Operation System	Release
CentOS distribution	8.2-2004
Kernel	4.18.0-227.el8.x86_64
Kernel-Realtime	4.18.0-227.rt7.39.el8.x86_64
C/C++ Toolkit	**Release**
Gcc-toolset	9.0
GNU GCC	9.2.1
googletest	1.10.0
cppcheck	2.3
valgrind	3.15.0
cpplint	1.4.5
aravis	0.7.5
boost	1.75
OpenBLAS	0.3.9
Open62541	1.2.2
aravis	0.7.5

waf	2.0.23
protobuferr	3.6.0
Java Toolkit	**Release**
Java OpenJDK	1.8.0_262
testNG	6.12
findbugs	3.0.1
checkstyle	7.1.1
Python Toolkit	**Release**
Anaconda Distribution	4.8.3
python	3.7.6
scipy	1.4.1
numpy	1.18.5
astropy	4.0
pylint	2.4.4
ipython	7.13.0
GUI Toolkit	**Release**
QT5	5.14.0
PyQt5	5.9.2
pyside2	5.14.1
Integration Software	**Release**
IDE Eclipse (Eclipse)	4.16
doxygen	1.8.20
robotframework	4.1
puppet	6.9.0
git	2.18.4
subversion	1.10.2
consul	1.8.19
lmod	8.2.7
nomad	0.12
wireshark	3.2.5
Other Software	**Release**
ptp, ntp	
tcpdump, perf, iperf, netcat	

systemtap, strace, sysdig	
pcp, atop, htop	

10.2 Register of Accepted Standard Hardware Products

10.2.1 PLC Technologies

[R-CSD-398] / / /
The register AD06 covers the PLC-related hardware applicable for use in control system construction.

10.2.2 National Instruments Technologies

[R-CSD-400] / / /
The following register covers chassis and controllers from National Instruments.

Any PXI system in the EELT will have to have a controller and one synchronization card (PXI-6683 or PXI-6683H), therefore 4 slots chassis are discouraged.

No product classified by National Instruments as a “Legacy Product” shall be included.

All cRIO power supplies shall be 24V DC.

PXI Chassis
NI PXIe-1085
NI PXIe-1066DC
NI PXIe-1082
NI PXIe-1075
NI PXIe-1065
NI PXIe-1062Q
NI PXI-1044
NI PXI-1045
NI PXI-1042
NI PXI-1042Q
NI PXIe-1078
NI PXIe-1071
NI PXI-1056
NI PXI-1036
NI PXI-1050
NI PXI-1052
PXI Controllers
NI PXIe-8135

NI PXIe-8100 RT
NI PXIe-8135 RT
NI PXI-8119
NI PXI-8119 RT
NI PXIe-8135 with removable HDD option
NI PXIe-8880
NI PXIe-8840
NI PXIe-8840 RT
NI PXI-8840
NI PXI-8880
cRIO Chassis
NI 9147
NI 9149
NI cRIO-9118
NI cRIO-9116
NI cRIO-9114
NI cRIO-9113
NI cRIO-9112
NI cRIO-9111
NI 9144
cRIO Controllers (integrated)
NI cRIO-9065
NI cRIO-9064
NI cRIO-9063
NI cRIO-9066
NI cRIO-9067
NI cRIO-9030
NI cRIO-9031
NI cRIO-9033
NI cRIO-9035
NI cRIO-9036
NI cRIO-9038
cRIO Controllers (embedded)
NI cRIO-9025
NI cRIO-9024
NI cRIO-9023
NI cRIO-9022
NI cRIO-9014

NI CRIO-9012