INTERNATIONAL STANDARD

ISO 21442

First edition
2022-05

Space systems — General requirements for control engineering

Systèmes spatiaux — Exigences générales relatives aux techniques de régulation

Reference number
ISO 21442:2022(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 20, *Aircraft and space vehicles*, Subcommittee SC 14, *Space systems and operations*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

The development of control systems applied to space systems requires cooperation among multi-disciplinary technology fields. A control system is often comprised of a large system integration of these technology fields. The development also requires cooperation with higher-level systems and the systems engineering method.

The purpose of this document is to provide general requirements for the entire life cycle in control systems development including the systems engineering method required for developing control systems applicable to space systems. Control engineering refers to systematic activities using systems engineering methods to realize the control system. The concepts, methods and models of system engineering are also applicable to control engineering. This document focuses on the special requirements of control engineering.

The development of a control system involves important aspects of system engineering, electrical and electronic engineering, mechanical engineering, software engineering, communications, ground systems and operations – all of which have their own dedicated standards. This document does not intend to duplicate them.

This document focuses on the specific issues involved in control engineering and is intended to be used as a structured set of systematic engineering provisions, referring to the specific standards and handbooks of the discipline where appropriate. For this and given the very rapid progress of control component technologies and associated "de facto" standards, this document does not go to the level of describing equipment or interfaces. Specific project or program standards are prepared for these purposes.

This document is not intended to replace textbook material on control systems theory or technology; and such material is intentionally avoided. The users of this document are assumed to possess general knowledge of control systems engineering and its applications to space missions.

Space systems — General requirements for control engineering

1 Scope

This document deals with control systems developed as part of a space project. It is applicable to all the elements of a space control system, including the space segment, the ground segment and the launch service segment.

This document establishes general principles for all technical activities of space control engineering, including control engineering management, requirements definition, analysis, design, production, verification and validation, operation, maintenance, and disposal. It also provides requirements to progressively refine and manage control system realizations in space systems including multiple control systems.

The requirements of this document can be tailored for each specific space program application.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 14300-1, *Space systems — Programme management — Part 1: Structuring of a project*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
activity
set of cohesive *tasks* (3.26) of a *process* (3.21)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.3]

3.2
actuator
component that performs the moving function of a mechanism

Note 1 to entry: An actuator can be either an electric motor, or any other mechanical (e.g. spring) or electric component or part providing the torque or force for the motion of the mechanism.

[SOURCE: ISO 26871:2020, 3.1.1]

3.3
control
purposeful action on or in a *process* (3.21) to meet specified objectives

Note 1 to entry: Control includes function of the *controller* (3.14) to derive *control commands* (3.4) to match the current or future estimated state with the desired state.

[SOURCE: IEC 60050-351:2013, 351-42-19, modified — The original notes to entry has been replaced by a new note 1 to entry.]

3.4
control command
output of the *controller* (3.14) to the *actuators* (3.2) and the *sensors* (3.24)

Note 1 to entry: This definition is applicable in case of sensors with command interfaces.

3.5
control component
element of the *control system* (3.12) which is used in part or in total to achieve the *control objectives* (3.9)

3.6
control engineering
systematic *activities* (3.1) using systems engineering methods to realize the *control system* (3.12)

3.7
control function
group of related *control* (3.3) actions (or *activities* (3.1)) contributing to achieving some of the *control objectives* (3.9)

Note 1 to entry: A control function describes what the *controller* (3.14) does, usually by specifying the necessary inputs, boundary conditions and expected outputs.

3.8
control mode
temporary operational configuration of *control systems* (3.12) implemented through a unique set of *sensors* (3.24), *actuators* (3.2) and *controller* (3.14) algorithms acting upon a given *controlled plant* (3.11) configuration

3.9
control objective
goal that the *controlled system* (3.13) is supposed to achieve

Note 1 to entry: Control objectives are issued as requests to the *controller* (3.14), to give the *controlled plant* (3.11) a specified *control performance* (3.10) despite the disturbing influences of the environment. Depending on the complexity of the control problem, control objectives can range from very low-level commands to high-level mission goals.

3.10
control performance
quantified capabilities of a *controlled system* (3.13)

Note 1 to entry: The control performance is usually the quantified output of the *controlled plant* (3.11).

Note 2 to entry: The control performance is shaped by the *controller* (3.14) through *sensors* (3.24) and *actuators* (3.2).

3.11
controlled plant
plant
physical system, or one of its parts, which is the target of the control problem

Note 1 to entry: The control problem is to modify and shape the intrinsic behaviour of the controlled plant such that it yields the *control performance* (3.10) despite its (uncontrolled other) interactions with its environment.

3.12
control system
part of a *controlled system* (3.13) which is designed to give the *controlled plant* (3.11) the specified *control objectives* (3.9)

Note 1 to entry: This includes all relevant functions of *controllers* (3.14), *sensors* (3.24) and *actuators* (3.2).

3.13
controlled system
control (3.3) relevant part of a system to achieve the specified *control objectives* (3.9)

Note 1 to entry: This includes the *control system* (3.12) and the *controlled plant* (3.11).

3.14
controller
control component (3.5) designed to give the *controlled plant* (3.11) a specified *control performance* (3.10)

Note 1 to entry: The controller interacts with the controlled plant through *sensors* (3.24) and *actuators* (3.2). In its most general form, a controller can include hardware, software, and human operations. Its implementation can be distributed over the space segment and the ground segment.

3.15
dependability
<of an item> ability to perform as and when required

Note 1 to entry: Its main components are *reliability* (3.22), availability and *maintainability* (3.17).

Note 2 to entry: The extent to which the fulfilment of a required function can be justifiably trusted.

Note 3 to entry: Dependability shall be considered in conjunction with *safety* (3.23).

Note 4 to entry: Dependability is used as a collective term for the time-related quality characteristics of an item.

[SOURCE: ISO 10795:2019, 3.80]

3.16
guidance
function of the *controller* (3.14) to define the current or future desired state

Note 1 to entry: This term is used as in guidance and *navigation* (3.18) *control system* (3.12) (GNC).

Note 2 to entry: GNC and attitude and orbit control systems (AOCS) or are often decomposed as two separate subsystems.

3.17
maintainability
<of an item> ability to be retained in, or restored to a state in which it can perform as required, under given conditions of use and maintenance

Note 1 to entry: Given conditions of use may include storage.

Note 2 to entry: Given conditions of maintenance include the procedures and resources for use.

Note 3 to entry: Maintainability may be quantified using such measures as mean time to restoration, or the probability of restoration within a specified period of time.

[SOURCE: ISO 10795:2019, 3.144]

3.18
navigation
function of the *controller* (3.14) to determine the current or future estimated state from the measured state

Note 1 to entry: This term is used as in *guidance* (3.16) and navigation *control system* (3.12) (GNC).

3.19
operability
feature of the spacecraft itself that enables a specified ground segment to operate the space segment during the complete mission lifetime of the spacecraft

[SOURCE: ISO 14950:2004, 3.1.7, modified — Note 1 to entry has been removed.]

3.20
pointing control
function of determining the direction of the *controlled plant* (3.11), turning toward a target, and remaining fixed on that target

3.21
process
set of interrelated or interacting *activities* (3.1) that use inputs to deliver an intended result

[SOURCE: ISO 9000:2015, 3.4.1, modified — Notes to entry have been removed.]

3.22
reliability
ability of an item to perform a required function under given conditions for a given time interval

[SOURCE: ISO 10795:2019, 3.198, modified — Notes to entry have been removed.]

3.23
safety
state where an acceptable level of risk is not exceeded

Note 1 to entry: Risk relates to:

— fatality,

— injury or occupational illness,

— damage to launcher hardware or launch site facilities,

— damage to an element of an interfacing crewed flight system,

— the main functions of a flight system itself,

— pollution of the environment, atmosphere or outer space, and

— damage to public or private property.

[SOURCE: ISO 10795:2019, 3.210, modified — "manned" has been changed to "crewed".]

3.24
sensor
device that measures states of the *controlled plant* (3.11) and provides them as feedback inputs to the *controller* (3.14)

3.25
simulation
use of a similar or equivalent system to imitate a real system, so that it behaves like or appears to be the real system

[SOURCE: ISO 16781:2021, 3.1.9]

3.26
task
required, recommended, or permissible action, intended to contribute to the achievement of one or more outcomes of a *process* (3.21)

[SOURCE: ISO/IEC/IEEE 15288:2015, 4.1.50]

4 Abbreviated terms

CE	control engineering
EGSE	electrical ground support equipment
FDIR	fault detection, isolation and recovery
H/W	hardware
ICD	interface control document
SE	system engineering
S/W	software
V&V	verification and validation
TM/TC	telemetry-telecommand
TRL	technology readiness levels
TT&C	telemetry, tracking and control

5 Control engineering

5.1 The general control structure

To illustrate and delineate the scope of CE, Figure 1 shows a general control structure.

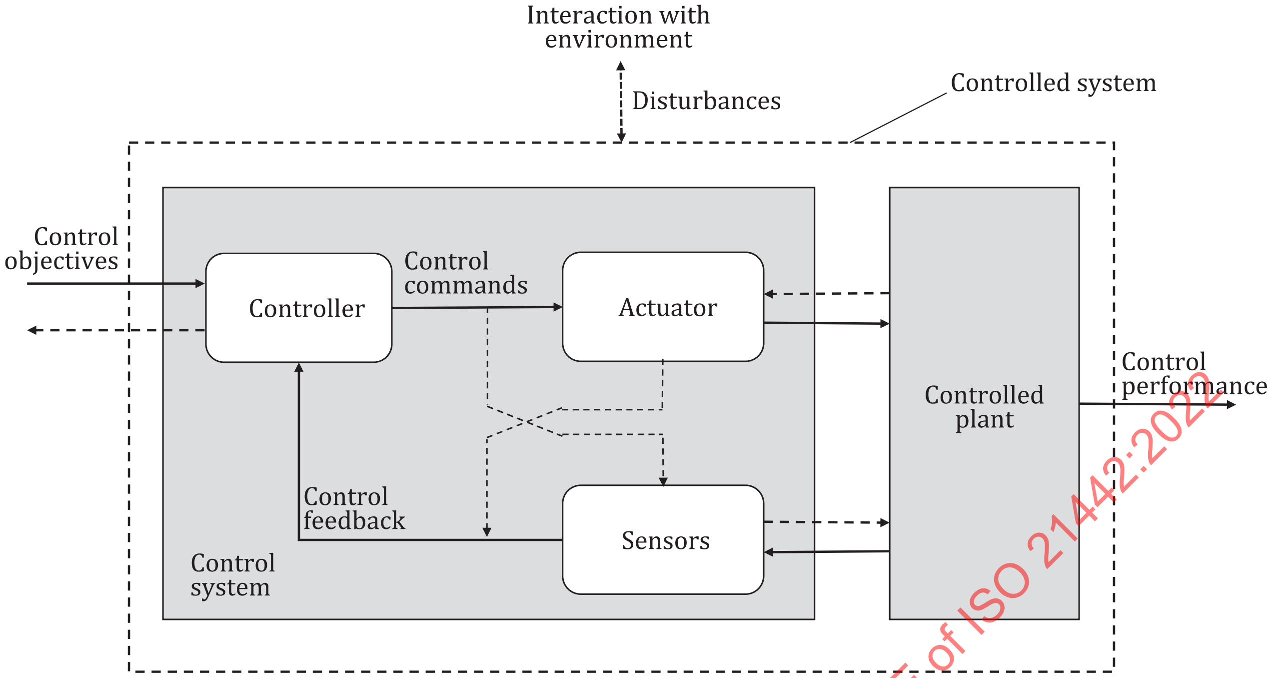

Figure 1 — General control structure

CE, as applied to control system development, in which performance and functional requirements and trade-offs are allocated aspects of top-level systems design, performs in close cooperation with systems engineering as specified in ISO 18676. CE aims at hands-on guidelines for developing the control system, while SE is common for any technical field.

The controlled system can be realized as multiple instantiations of the general control structure. Control engineering activities specified in this document are implemented for developing a control system controlling each controlled target, and those activities are integrated within the controlled system development.

Control system always includes some kind of feedback loop. The intrinsic behaviour and output of the controlled plant do not meet the expectations without being modified and shaped. For space applications, the controlled plant can be:

a) satellite (its attitude, orbit) or a cluster of satellites;

b) spacecraft during re-entry, landing, rendezvous or docking;

c) pointing control system;

d) robot arm system;

e) rover;

f) automation of payload and experiment facility;

g) launch vehicle;

h) any other technical system involving feedback control.

5.2 Project phases

As defined in ISO 14300-1, to minimize the technical, scheduling and economical risk of the project, and to make the progress of the project being controlled, the product life cycle shall be divided into distinct phases which are interlinked.

The phases of a project are listed in Table 1.

Table 1 — Phases of a project

Index	Name
Phase 0 or pre-phase A	Mission analysis phase
Phase A	Feasibility phase
Phase B	Definition phase
Phase C	Development phase
Phase D	Production phase
Phase E	Utilization phase
Phase F	Disposal phase

During phase 0, CE makes an initial definition about the mission of control system development and makes a preliminary assessment of the concepts needed for consideration in the next phase (phase A).

During phase A, CE explores various possible control system schemes, so as to meet the requirements requested by the spacecraft system for the control system, including performance, cost and schedule.

During phase B, CE selects one proposal for development among those proposed at the end of the previous phase (phase A) and specifies the necessary requirements.

During phase C, CE conducts a detailed study of the proposal of the previous phase (phase B), so as to obtain a qualified solution of control system for mass production of deliverable products for operation.

During phase D, CE accomplishes procurements, manufacture and delivery to the user the control system. For scheduling reasons, some procurement may be started prior to phase D.

Phase C and phase D may be merged into one unique C/D phase if the project leads to the manufacturing of a single-flight unit or of a very small quantity of product.

During phase E, the control system is properly operated and maintained, thus it is put into service, used and supported.

During phase F, CE prepares and completes the discontinuance of control system operation, in accordance with other systems of the spacecraft.

The number of phases and their objectives should be defined at the start of the project. They should also be tailored to minimize risks from cost, scheduling and technical problems that can compromise the success of the project.

5.3 Control engineering process

The CE process itself employs many of the same elements as the SE process to achieve precision performance, dynamic responsiveness, default isolation, control ability, and functional and non-functional goals. As such, it can also be broken down into some engineering activities:

a) control engineering management, which integrates the various control related disciplines throughout all project phases to define and realize the controlled system;

b) requirements definition, which includes proper interpretation of the mission, control requirements, and definition of lower-level requirements;

c) analysis, performed at all levels and in all domains for resolving control related functional and performance requirements, evaluating control design alternatives; consolidating and verifying control performances and complementing tests;

d) design, which includes interface design, algorithm design, software design and integrated design;

e) production, which includes procurement, manufacturing, screening, acceptance, storage, transportation and package;

f) V&V, to demonstrate, through a dedicated process, that the control system meets its control objectives and requirements; testing is an important method of V&V; it mainly includes software test, equipment (controller, sensors and actuators) test, subsystem test and integrated test;

g) operation, which includes ground operations and space operations, intending to retain the controlled system in, or restore it to, a state in which it can perform as required;

h) maintenance, which includes equipment maintenance and software maintenance;

i) disposal, in which the controlled system or controlled system components are deactivated and removed from operations.

These different CE activities are, at various phases of the control system development, conducted to support one another in the proper development of the control system. These interactions are shown in Figure 2.

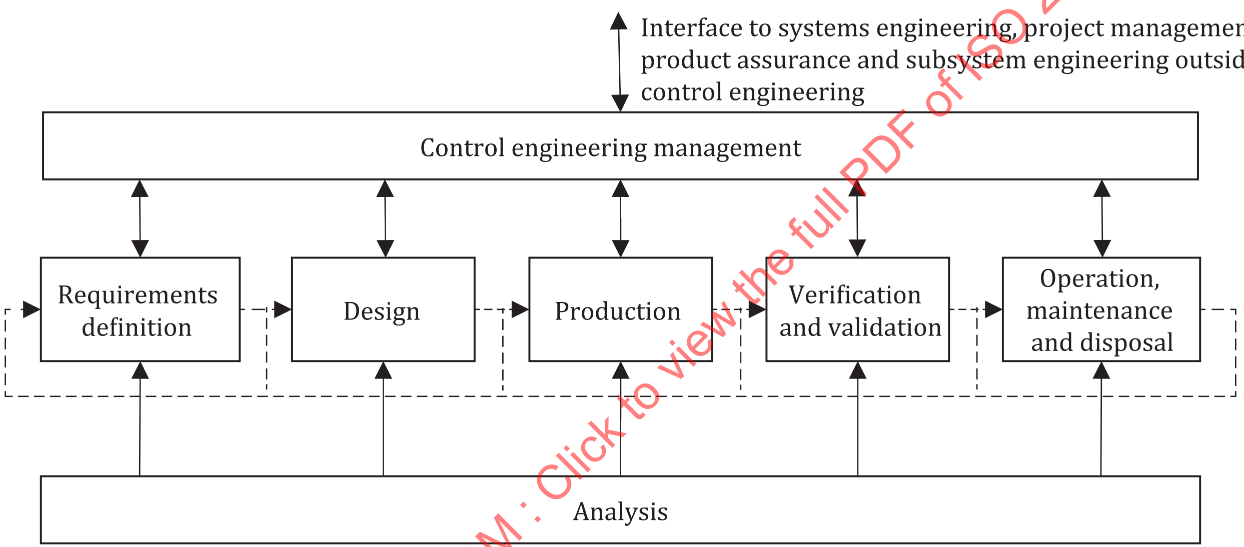

Figure 2 — Interaction between CE activities

In the activity of control engineering management, the organization and plan of the control system are established, including the tasks in each process, interfaces with other disciplines, budget plan, technology readiness level and cost effectiveness assessment, risk management, change control and configuration management, capability assessment and resource management.

In the activity of requirements definition, the requirements from upper level are reasonably decomposed to obtain the requirements for the control system, and further decomposed into the requirements for each component of the control system. The decomposition of these requirements is based on qualitative or quantitative analysis.

In the activity of design, conceptual design or detailed design of control system architecture, algorithm, software, components and interfaces are carried out according to the results of requirements definition. In the design process, it is necessary to perform an analysis to obtain compromise or optimization results, and to validate and verify the temporary or formal design results to ensure that the design results meet the requirements. The activities of design, analysis and V&V usually need to be iterated for many times.

After obtaining the design results, the production of the control system, including procurement, manufacturing, screening, inspection and other tasks, is conducted. The obtained control system is assembled on the spacecraft for validation flight test or put into practical use.

Operation and maintenance for control system are conducted on the ground or in flight.

Disposal deals with actions of moving a space system to a new orbit that causes the space system to be removed from the region in outer space that is protected with regard to the generation of space debris to ensure its safety and sustainable use in the future.

The tasks of each activity of CE are summarized in Table 2.

Table 2 — Tasks of CE activities

CE activity	CE tasks
Control engineering management	— Organization and planning of control engineering activities — Management of interfaces with other disciplines (e.g. mechanical engineering and software engineering) and activities (e.g. procurement and quality assurance) — Contribution to human factors engineering when humans are part of the controller — Definition of budget and margin philosophy for control — Assessment of control technology and cost effectiveness — Risk management — Engineering support to control components procurement — Change control and configuration management — Control engineering capability assessment and resource management — System safety — Dependability management — Quality assurance
Requirements definition	— Generation of control requirements from space system and mission — Allocating control requirements to control components (sensors, actuators, control H/W and S/W)
Analysis	— Definition of analysis models — Selection of adequate analysis methods and analysis tools — Control system requirements analysis — Control system disturbance analysis — Control system performance analysis, such as error budget analysis, stability analysis and robustness analysis — Verification analysis
Design	— Control system architecture design — Control system functional design — Control system interface design — Control algorithm design — Control system software design — Control system configuration design — Control system implementation and operational design
Production	— Manufacturing, assembly and integration

Table 2 *(continued)*

CE activity	CE tasks
Verification and validation	— Definition of control verification strategy — Preliminary verification of performance by analysis or prototyping — Final functional and performance verification by analysis — Final verification and validation of controlled system by hardware-in-the-loop tests — In-flight validation of controlled system behaviour
Operations	— On-ground operation — In-space operation
Maintenance	— Equipment maintenance — Software maintenance
Disposal	— Required engineering support for disposal operations including de-orbit.

At different project phases, the requirements of CE activities can be tailored according to the specific attribute and needs. Tailoring guidelines are shown in Annex A.

5.4 Control engineering tasks per project phase

The primary control engineering tasks to be performed at each phase of the project, and the inputs, the tasks and the outputs for each activity are shown in Table 3 to Table 6.

Table 3 — Control engineering inputs, tasks and outputs, phase 0/A

Phase 0/A	Control engineering management	Requirements definition	Analysis	Design	Production	Verification and validation	Operation, maintenance and disposal
Inputs	— Control system development schedule — Control system development approach and constraints	— System objectives — Mission requirements — Control system performance requirements	— Controlled system objectives — Preliminary control system requirements	— Control system design concepts of similar space systems	— Control system production requirements	— Control system verification and validation approach	— Operation, maintenance and disposal requirements
Tasks	— First assessment of control system development cost and schedule — Generation of inputs to control system development approach — Identification of availability and maturity of control technology	— Translate mission and system objectives into preliminary control objectives — Definition of preliminary control requirements — Definition of control system life cycle	— Analysis of control requirements feasibility for control system alternatives — Preliminary disturbances evaluation — Preliminary performance assessment	— Establishment and trade-off of control system design concepts — Establishment of control system design baseline (including preliminary FDIR concept)	— Requirements analysis and feasibility analysis of manufacturing resources — Requirements analysis and feasibility analysis of manufacturing technology	— Control engineering support for definition of verification and validation concepts — Preliminary definition of control verification and validation methods and strategies	— Translate operation, maintenance and disposal requirements into preliminary control objectives
Outputs	— Inputs to project and control system engineering plan — Inputs to cost and schedule estimates — Inputs to technology development plan	— Inputs to control system requirements documentation	— Control system analysis report	— Preliminary control system design and analysis report	— Inputs to feasibility analysis report	— Inputs to development and verification planning	— Inputs to control system requirements documentation

Table 4 — Control engineering inputs, tasks and outputs, phase B

Phase B	Control engineering management	Requirements definition	Analysis	Design	Production	Verification and validation	Operation, maintenance and disposal
Inputs	— Phase 0/A project planning and cost estimates — Control life cycle phase 0/A	— System objectives — Mission requirements — Controlled system objectives and requirements	— Phase 0/A simulation models — Phase 0/A control analysis	— Phase 0/A control design	— Control system production requirements	— Control system verification plan — Phase 0/A control verification plan	— Operation, maintenance and disposal requirements
Tasks	— Update control system inputs to system engineering management plan and cost estimates (including risk management) — Review of the control systems compatibility with the system design and constraints	— Analyse system requirements — Generate controlled system requirements — Allocate controlled system requirements to subsystems and components — Check traceability of control requirements with respect to system requirements	— Analysis of control requirements for sub-systems and components — Disturbances assessment — Controlled system performance analysis — Assessment of control technologies for early prototyping	— Definition of control system baseline — Allocation of control system functions to H/W, S/W and human operators (in-flight and on ground) — Definition of control system interfaces — Preliminary design of controller (control laws) — Selection of control components and technologies	— Preliminary plan of control system manufacturing resources	— Prepare controlled system verification plan — Provide inputs to lower-level verification plans — Support phase C/D verification planning	— Analyse operation, maintenance and disposal requirements
Outputs	— Inputs to project and system engineering plan — Inputs to cost estimates and schedule	— Inputs to system or subsystem technical specifications — Inputs to lower-level technical specifications	— Controlled system analysis report (including simulation models description)	— Control system design report (including design justification) — Preliminary control algorithms specification	— Inputs to control system plan	— Controlled system verification plan — Preliminary controlled system verification report	— Inputs to system or subsystem technical specifications

Table 5 — Control engineering inputs, tasks and outputs, phase C/D

Phase C/D	Control engineering management	Requirements definition	Analysis	Design	Production	Verification and validation	Operation, maintenance and disposal
Inputs	— Phase B project planning and cost estimates — Phase B control life cycle	— Phase B control objectives and requirements — Phase B control components specifications	— Phase B simulation models — Phase B control analyses	— Phase B control design and design justification	— Phase B control system production requirements	— Phase B controlled system verification plan	— Operation, maintenance and disposal requirements — System or subsystem technical specifications
Tasks	— Support of control system engineering and project management (including risk management) — Management of required control system changes — Support to phase E/F planning and cost estimate	— Update of specifications — Review and assessment of control requirements change — Review and assessment of system changes related to control	— Detailed controlled system performance analysis — Support to verification process — Support to in-flight verification process definition	— Update of the control design baseline — Finalization of control system functional architecture and interfaces — Detailed design of controllers and optimization of controller parameters	— Procure control system components — Manufacture control system components — Software production — Inspect products quality — Store, transport and package of control system products — Support to storage, transportation and package — Support to assembly and test of spacecraft	— Co-ordinate and monitor controlled system and lower-level verification plans and activities — Monitor lower-level verification acceptance activities — Support and monitor lower-level qualification and acceptance tests — Perform controlled system qualification and acceptance tests	— Generation of operation, maintenance and disposal document

Table 5 *(continued)*

Phase C/D	Control engineering management	Requirements definition	Analysis	Design	Production	Verification and validation	Operation, maintenance and disposal
Outputs	— Updated inputs to project and control system engineering plan — Updated inputs to cost estimates for phase E/F	— Updated inputs to system or subsystem technical specifications — Updated inputs to lower-level technical specifications — Updated inputs to interface control documents	— Controlled system analysis report — Inputs to the definition of the strategies for the in-flight calibration and performance analysis	— Final control system design report — Final control algorithms specification (including control system TM/TC specification)	— Delivered control system and relating documents	— Controlled system verification report — Inputs to in-flight verification plan	— Operational document — Disposal specification

Table 6 — Control engineering inputs, tasks and outputs, phase E/F

Phase E/F	Control engineering management	Requirements definition	Analysis	Design	Production	Verification and validation	Operation, maintenance and disposal
Inputs	— System operations planning	— Final system and lower-level specifications	— Controlled system requirements — Controlled system in-flight performance data — Strategies for the in-flight performance analysis	— Final control system design report	— Control system production report	— In-flight verification plan	— Operation maintenance document — Disposal specification
Tasks	— Support of system operations — Management of specified controller changes — Control engineering support to system disposal — Generation of lessons learnt for control engineering	— Comparison of control objectives and requirements with controlled system performance — Clarify control objectives and requirements changes during operation	— Analysis of controlled system operational performance — Analysis of required controller changes	— Update of controller design (in case of required changes)	— Spare components production if necessary	— Support controlled system operational performance verification — Support system review	— Support of operation, maintenance and disposal — Perform disposal
Outputs	— Inputs to disposal plan	— New control related operational requirements	— Inputs to controlled system operational performance report — Updated controlled system analysis report — Inputs to payload data evaluation	— Controller design updates (updated control system design report)	— Spare components	— Inputs to in-flight acceptance report — Inputs to periodic mission reports	— Operational report — Operational record — Maintenance record — Disposal report — Disposal record

6 Control engineering process requirement

6.1 Control engineering management

6.1.1 General

The control engineering management activities contribute to system engineering from a control engineering point of view and support the system engineering management activities. Therefore, control engineering management activities interface with the activities of the project stated in ISO 14300-1.

It shall be consistent with the system engineering management plan and system engineering management requirements.

6.1.2 Organization and planning of control engineering activities

Control engineering management plan defines, organizes and plans all control engineering activities to achieve the specified control performance. It applies to the control development and verification logic which is related to the system design and development planning.

Control engineering shall participate in all major project reviews to assess the system design and system design changes from the control point of view.

6.1.3 Management of interfaces with other disciplines

Control engineering provides inputs and review related system parameters, constraints and interfaces, including:

— electrical interfaces;

— mechanical interfaces;

— thermal interfaces;

— software interfaces;

— ground segment interfaces;

— operational interfaces;

— TT&C interfaces;

— optical.

The control related system parameters, constraints and interfaces shall be approved at system level.

6.1.4 Contribution to human factors engineering

Control engineering contributes to human factors engineering in the case when humans are part of the control loop. The following factors are typically considered:

— human performance capabilities;

— man-machine interfaces;

— training of control operators.

6.1.5 Budget and margin philosophy for control

For control related budgets with several contributors, summation rules are defined and used consistently throughout the design process. A margin policy is established and applied. Budget methodology and margin philosophy can evolve during the development according to the level of maturity of the control system.

6.1.6 Assessment of control technology and cost effectiveness

The programmatic risk concerning the maturity of the control related technology is assessed and analysed, especially with respect to the controller, sensors and actuators. The effort (cost and risk) for the verifications of the control objectives and requirements is also assessed.

6.1.7 Risk management

Control engineering risk analysis shall be performed from a technical point of view.

NOTE ISO17666 is available for this activity.

6.1.8 Support to control components procurement

Control engineering supports system engineering for the procurement of the controller, sensors and actuators.

6.1.9 Change control and configuration management

Control engineering supports the management of non-conformances related to control, handles changes related to controller design and implementation, and reviews changes in control related disciplines. Configuration items of control system are identified and managed.

NOTE ISO 10007 or ISO 21886 are available for this activity.

6.1.10 Control engineering capability assessment and resource management

Control engineering assesses the control related capability and experience, and performs the related resource management.

6.1.11 System safety

The programme management concerning system safety shall be performed in the control engineering management process.

NOTE ISO 14620-1 is available for this activity.

6.1.12 Dependability management

Dependably management shall be performed in the control engineering management process.

NOTE ISO 23460 is available for this activity.

6.1.13 Quality assurance

Quality assurance shall be performed in the control engineering management process.

NOTE ISO 27025 is available for this activity.

6.2 Requirements definition

6.2.1 General

The requirements to the control system from mission shall be defined according to the expectation of mission, such as function, cost, and dependability. The requirements to the control system shall consider constraints imposed from other systems, such as electrical power, mechanical configuration, thermal conditions and operation.

The requirements to the control system are allocated to lower-level requirements for the control components (controller, sensors and actuators).

The allocation of requirements to lower levels shall be normally iterative process and performed repeatedly.

6.2.2 Generation of control requirements

The control requirements are derived from the directly applicable system requirements, taking into account constraints imposed by other system requirements (e.g. electrical power, mechanical configuration, thermal conditions and operations).

The generation of control requirements maintains traceability and justification of the control requirements. Control requirements shall be specified so that the conformity with system requirements can be checked.

Beside the top-down style, the generation of control requirements can also take into account the bottom-up style, for example, from the reuse of existing equipment and control law elements.

Control requirements shall be documented (such as specifications, design conditions, ICD) and authorized. Special system constrains to control system (such as minimum allowable thruster tilt angle for plume effect limitation, sensor field of view, actuator operating range, alignment, mechanical stiffness, eigenfrequencies) shall be documented as proper documents.

Control requirements include the following requirements:

a) functional requirements, e.g. attitude stabilization and manoeuvre, orbit manoeuvre and orbit maintaining;

b) performance requirements, e.g. guidance and orbit control precision, attitude control stability, and electrical performance;

c) mission peculiar requirements, e.g. collision avoidance during mission, deorbit, reorbit, minimum allowable thruster tilt angle for plume effect limitation, sensor field of view, actuator operating range, alignment, mechanical stiffness, eigenfrequency;

d) other requirements, e.g. physical constraints (mass, electrical power consumption), dependability, mission safety, cost constraints, schedule constraints.

6.2.3 Allocation of control requirements to control components

6.2.3.1 General

This subclause provides a checklist of the requirements to be identified and defined by CE for any control component. The level of detail depends on the phase of the project.

All properties of the control components can be checked for feasibility.

6.2.3.2 Sensors

The following sensor properties can be defined:

a) functional and performance requirements (possibly specified separately for the different modes):

— measurement principle (analogue-digital);

— absolute-relative accuracy (before-after calibration);

— measurement range (including limitations imposed by operating conditions);

— resolution;

— linearity;

— maximum allowed unpredictable bias;

— measurement bandwidth;

— timing requirements (e.g. sampling rate, maximum delay time, and maximum time jitter for sampling rate and delay);

— maximum allowed noise, including quantization noise from analogue/digital conversion;

— FDIR requirements.

b) operational requirements:

— measurement modes (e.g. fine mode or coarse mode);

— conditions for mode transitions;

— operational restrictions (e.g. solar exclusion angle for an optical sensor and recovery after blinding);

— calibration requirements: type (permanent or occasional), frequency, duration and parameters to refresh;

c) configuration requirements:

— accommodation requirements (e.g. free field of view, and minimum stiffness between actuators and sensors);

— disturbance constraints from internal sources (e.g. vibrations);

d) interface requirements:

— alignment requirements (bias and stability);

— electrical interface requirement (e.g. maximum noise for analogue interfaces);

— data interface requirement (e.g. resolution);

e) verification requirements:

— test interface requirements (stimuli inputs);

— special provisions for ground testing.

6.2.3.3 Actuators

The following actuator properties can be defined:

a) functional and performance requirements (possibly specified separately for the different modes):

— actuation principle;

— absolute-relative accuracy (before-after calibration);

— operating range (including limitations by operating conditions);

— resolution;

— linearity;

— maximum allowed unpredictable bias;

— actuation bandwidth for various defined control command points, response time and settling time (step response);

— timing requirements (e.g. command rate, maximum delay time, and maximum time jitter for sampling rate and delay);

— maximum allowed noise, including quantization noise from digital/analogue conversion;

— FDIR requirements;

b) operational requirements:

— actuation mode (e.g. torque or speed control);

— conditions for mode transitions;

— operational restrictions (e.g. maximum number of actuators);

— calibration requirements: type (permanent or occasional), frequency, duration and parameters to refresh;

c) configuration requirements:

— accommodation requirements (e.g. position and orientation of actuator);

— avoidance of disturbances caused by actuator;

d) interface requirements;

— alignment requirements (bias and stability);

— electrical interface requirement (e.g. maximum noise for analogue interfaces);

— data interface requirement (e.g. resolution);

e) verification requirements:

— testing interface requirements (stimuli outputs);

— special provisions for ground testing.

6.2.3.4 Controller hardware requirements

The following requirements for the controller hardware can be defined:

a) sampling rates for sensor reading;

b) sampling rates for actuator commanding;

c) sampling rates for controller functions;

d) allowed processing delays for reading sensor information, controller processing and actuator commanding;

e) allowed time jitter in delays;

f) electrical interface requirements (including requirements for anti-aliasing filters);

g) requirements on computational performance and memory size.

NOTE The actual code size and processor load depend very much on the implementation of the control software. The detailed definition of these parameters can only be done together with the control software design.

6.2.3.5 Controller software requirements

The following requirements for the controller software can be defined:

a) algorithms for control functions to be implemented in the controller;

— definition of desired state;

— determination of estimated state;

— derivation of control commands;

— control mode management;

— control system status monitoring;

— FDIR;

b) precision for the calculation of the control algorithms;

c) control software timing conditions (sampling rates, delays and jitter) in a consistent way together with the controller hardware timing conditions;

d) requirements for safety critical control functions;

e) control software interface requirements:

— from-to sensors and actuators;

— from-to system level control (on-board or ground).

6.3 Analysis

6.3.1 General

Analysis is a fundamental activity (based on models) performed in all phases of the control system development for the purpose of:

a) supporting the allocation of requirements among the different control functions;

b) substantiating the selection of control functional or physical architectures and implementations;

c) trading off alternative control solutions;

d) identifying design risk factors;

e) verifying the controlled system performance relative to its requirements and within the applicable environment.

Analysis contributes to the whole CE process. The analysis process interacts strongly with all the other CE activities.

6.3.2 Analysis models, analysis methods and analysis tools

6.3.2.1 Definition of analysis model

For analysis, proven models shall be used; and analysis models for mission and control system analysis shall be specified for control system interface conditions. The targets of modelling shall be all the components of a controlled system as shown in Figure 1, and shall include control system, controlled plants, and external environment.

According to the purpose of analysis and the phase of project, an adequate precision model shall be used; and the following models shall be defined as needed. The number of models and detailed specifications shall be determined in accordance with a project.

a) Simplified model

In the early project phases (phase 0, A and B), simplified analysis models are developed in order to allow preliminary control performance assessments.

These simplified models are used for providing inputs to control requirement feasibility evaluations and budget breakdown.

These simplified models are also used to support numerical trade-off for the evaluation of alternative control architectures, control concepts (algorithms) and selection among different control components.

b) Mathematical model

Mathematical model is mathematical description of the behaviour of the controlled plant, a control system component or the environment. This consists of algorithms, formulas and parameters. For performance analysis, mathematical models are developed and used. These models shall provide sufficient input and output data for the assessment of the control system performance. The number and detail of the models depend on the project phase.

c) Disturbance model

Disturbance means physical effect affecting the control performance that can act onto all components of the controlled system. The source of the disturbance can be internal (if generated inside the controlled system) or external (if coming from the environment).

Typical internal disturbances include:

— imbalance of rotating mass;

— vibration of structure;

— motion of internal mass and friction.

Typical external disturbances include:

— solar pressure disturbance;

— aerodynamic disturbance;

— gravity gradient disturbance;

— Earth magnetic field disturbance;

— thruster misalignment disturbance.

For performance analysis, disturbance shall be modelled using verified parameters or parameters identified by dedicated tests.

d) Simulation model

Simulation model is the implementation of a mathematical model in an environment to calculate the behaviour of the model. It is usually implemented by use of a computer program.

In phase C and D, in order to verify and optimize the design of control system, detailed closed-loop simulation model shall be developed, in which all elements of the controlled system and disturbances are modelled. The simulation models shall be calculated with adequate numerical precision compatible with requirements of control performance.

e) Error sources

Errors can affect the accuracy of the control system. Therefore, error sources should be analysed through mathematical method and simulation. Typical error sources include:

— installation error of sensor and actuator;

— deviation of aerodynamic characteristics;

— random error and systematic error.

6.3.2.2 Analysis methods and analysis tools

According to each phase of CE, one analysis method or combination of two or more analysis methods should be selected and used. The validity of analysis tools shall be evaluated and managed in appropriate ways.

6.3.3 Requirements analysis

6.3.3.1 General

In requirements analysis, mission and control system analysis shall be supported in accordance with mission requirements and control system requirements. Analysis shall be used extensively; and the following activities shall be supported along with a hierarchical flow.

a) A higher-level mission objective, for example, customer needs, shall be broken down into feasible control objectives.

b) The topology of the controlled system, for example, linear or nonlinear, single input - single output or multi input - multi output, shall be analysed.

c) Quantitative requirements for controlled system shall be analysed.

d) Requirements for the controlled system shall be allocated to lower-level requirements for various control components (controller, sensors and actuators) and controlled plants as shown in Figure 1.

e) By analysis, the feasibility of the requirements allocated to various control components shall be assessed.

6.3.3.2 Support for mission analysis, system analysis and CE requirements analysis

In each phase of CE, analysis related to system requirements for orbit, attitude and pointing control, for which mission requirements or space system requirements directly become control system requirements, shall be supported; and based on the results, detailed control error budget shall be defined and used as input data to technical specifications of control components. Allocation of control error budget shall be supported by analysis. Also, in each phase, mission analysis and control system analysis of these system requirements shall be supported; and the compatibility between the analysis results and control system requirements shall be assessed.

6.3.3.3 Disturbance analysis

In CE, in accordance with the definition in Figure 1, analysis for defining external disturbances and internal disturbances to controlled system shall be supported.

Disturbances which originate in a controlled plant shall be defined based on control system requirements. When disturbances are control system requirements, disturbance analysis shall be implemented as control system analysis support; and the compatibility between the analysis results and control system requirements shall be assessed. Analysis shall be implemented with the degree of precision required in each phase of the project; however, it may be omitted if the robustness of control system against external and internal disturbances has been verified by worst-case analysis and so forth.

6.3.4 Control system performance analysis

6.3.4.1 General

Control system performance analysis shall be performed as part of control system design for determining the parameters which specify control system performance. Also, in each phase of the project, it shall be assessed whether consistency is ensured between the controlled system performance and the following requirements:

a) control objectives generated by mission and space system analysis from mission and space system requirements;

b) quantitative requirements defined by analysis for requirements analysis.

In initial phases (phase 0, A and B) of the project, simplified analysis models shall be developed to perform preliminary assessment of control performance, in order to assess the feasibility of control requirements, to make error budget breakdown, to support numerical trade-offs, to assess alternative control architecture and control concept (algorithm), and to select control components.

In later phases (phase C, D, E and F) of the project, detailed mathematical models shall be developed. Performance assessment shall be performed by simulation analysis and so on. It shall be reviewed whether functions and performances required for controlled system are satisfied.

6.3.4.2 Error budget analysis

The error source and error analysis methods shall be used to analyse the error for control objectives; and it shall be assessed whether the allocated requirements are satisfied.

6.3.4.3 Stability analysis and robustness analysis

Stability and robustness should be evaluated for parameter variation. The nominal model and disturbance shall be considered in assessing whether the allocated margin is satisfied.

Disturbance consists of internal disturbances and external disturbances. Internal disturbances originate from control system and controlled plants, while external disturbances originate from external environment.

6.3.4.4 Verification analysis

As finalized performance verification, performance analysis with mission operational scenarios shall be performed based on mathematical models; and the degree of achievement of control system requirements shall be assessed from the following viewpoints.

Different verification analysis tools should be used if needed, to avoid the dependence on analysis tools.

In phase C and D, verification of control system shall be performed with the optimized control system design. In the end of phase C, verification shall be performed by simulation analysis and so on. If there are backup mode and FDIR function, they shall be verified.

6.4 Design

6.4.1 Control system architecture design

While designing the control system architecture, comprehensive trade-off among technical requirements, schedule requirements, and full life cycle cost shall be implemented.

To determine reasonable control system solutions, technical advantages and engineering feasibility, application and adaptability of control system architecture, employment of mature technologies, and test and verification of the new technologies to be employed, shall be considered.

6.4.2 Control system functional design

The functional design process consists of a resolution of control objectives into control system functions. This is usually achieved through a top-down process.

CE defines a functional design, compatible with the control system functional analysis, and consisting of control system functions (and sub-functions) which collectively meet the control objectives.

The functional design covers both nominal and non-nominal situations as well as specific functions for testing and verification.

6.4.3 Control system interface design

Interface design shall include the interface between the internal equipment of the control system and the interface between the control system and other parts of spacecraft.

CE related interfaces shall be matched.

The following shall be included as interfaces with other fields:

a) electrical interface;

b) mechanical interface;

c) environmental interface;

d) software interface;

e) operational interface;

f) telemetry, track and command interface.

CE shall support human engineering activities in the case human are part of the control loop.

Result of interface design shall be specified in ICD.

6.4.4 Control algorithm design

6.4.4.1 General

The controller uses algorithms (mathematical or logical) to derive commands for the actuators, based on sensor measurements and commands to the controller (e.g. reference inputs). These control algorithms can be implemented in digital or analogue form.

The controller shall be designed such that the controlled system meets the specified performance requirements. The effects influencing the control loop (such as performance of the control components, dynamic behaviour of the controlled plant, and disturbances due to the environment) shall be taken into account.

Typical control algorithm design includes guidance and orbit control design, attitude control design, redundancy and fault tolerance method design, which are described from 6.4.4.2 to 6.4.4.4.

6.4.4.2 Guidance and orbit control design

Guidance and orbit control design shall be implemented mainly considering the following engineering activities and tasks:

a) conceptual architecture design, including feasibility analysis and design, control system index analysis and distribution, guidance system design, guidance strategy design, redundancy configuration design, and component indexes design;

b) navigation method design and guidance law design;

c) experiments design, including mathematical simulation experiment design, guidance system closed-loop simulation experiment design, initial alignment experiment design, and accuracy experiment design.

6.4.4.3 Attitude control design

Attitude control design shall be implemented mainly considering the following engineering activities and tasks:

a) control system architecture design, including control system composition design, control capability analysis, control system polarity design and component indexes design;

b) control law design, including control strategy design and control equation design;

c) control parameters design, including control system model linearization, control system deviation combination design and control system stability analysis;

d) experiment design, including simulation experiment model establishment, mathematical simulation experiment design and hardware-in-the-loop simulation experiment design.

6.4.4.4 Redundancy and fault tolerance method design

Redundancy and fault tolerance method shall be designed during both guidance and attitude control design. Fault modes should be analysed; and fault diagnosis method should be adopted. Redundancy method design typically includes redundancy information management design, fault diagnosis logic design, fault discrimination threshold design, redundant components switch strategy design, and fault information restructure design.

6.4.5 Control system software design

The software design should choose an appropriate life cycle model, such as the waterfall model, incremental model, spiral model, rapid prototype model.

Control system software design mainly includes control system requirement development, software requirement analysis, software design, software implementation and software test. Specific requirements are identified in control system specification documents which are generated by requirement definition process.

Control system software design related activities should meet the requirements defined in ISO/IEC/IEEE 12207.

6.4.6 Control system configuration design

Control system configuration (physical architecture) refers to a set of components (comprised of sensors, actuators, controllers, controlled plants, software and hardware) to be used to achieve control objectives. In control system design, CE shall take the limitation of these physical elements into account and achieve a feasible design. Furthermore, in CE, the physical characteristics of these components shall be applied to design controller. Since these operations often affect other domains and vice versa, it is expected that such operations on a complex system are in coordination with systems engineering. In configuration design, the configuration of sensors and actuators shall be determined to achieve all control objectives in terms of performance, redundancy, observability, controllability and operability.

6.4.7 Control system implementation and operational design

Implementation design of each control components shall be performed in accordance with the system design; and electrical and mechanical parts which are necessary for the implementation shall be designed. The design results shall be documented and managed as product specification, ICD and/or procedures, and so on. If there are subsystem-level requirements for verification, subsystem-level implementation and integration activities shall be performed in accordance with these documents; and verification at subsystem shall be performed. Also, if there are requirements from the system, control engineering should contribute to the system implementation.

Control systems implementation method into the operational system (e.g. implementation of on-board software, in particular, in-flight reprogramming), including verification methods, shall be coordinated with the system as interface design, and documented as ICD and/or operational manual. Also, if there are requirements from the system, documentation of implementation procedures into the operational system and system implementation support shall be performed.

6.5 Production

Production in control engineering, including manufacturing, assembly and integration, is a part of system production. Production related activities in control engineering should meet the requirements defined in ISO 18676.

6.6 Verification and validation

6.6.1 General

Verification and validation process in control engineering is a part of the system verification and validation process. Thus, it should be consistent with verification requirements defined in ISO 18676, ISO 23460 and ISO 27025.

The control objectives verification already starts from the earliest phase when possible concepts are identified and a control system concept is selected. An important part of the control objective verification is performed during the design engineering process when iterative checks are performed to make sure that requirements including margins are met. This is followed by verification of the actual hardware and software components of the control system. Hereafter, the different components are integrated and tested together, enabling verification at system level. Finally, as not all control performance requirements can be fully verified on the ground, additional verification can be performed in-flight.

Verification testing should be planned and performed according to ISO 15864.

6.6.2 Definition of control verification strategy

The strategy for the verification of the control objectives is defined in consistency with the system verification plan, and aims at demonstrating that all the controlled system requirements are met. In this frame, the control engineering verification process shall:

a) verify that the controlled system is capable of achieving the specified control objectives;

b) verify the design and performance of each part of the control system with respect to the allocated requirements;

c) verify that the flight hardware and software components of the control system conform to the requirements and are acceptable for use;

d) confirm controlled system integrity and performances after specified steps of the project life cycle (e.g. pre-launch and in-flight).

The effort of the verification of the control objectives shall be assessed according to the maturity of and flight experience with the controlled system design.

To implement the strategy, a plan for the verification and validation of the controlled system shall be developed and documented (possibly as part of the system verification plan). This plan includes:

— the logic between the different verification levels related to control (control component level, control system level and controlled system level);