ECSS-E-60A

14 September 2004

EUROPEAN COOPERATION

ECSS

FOR SPACE STANDARDIZATION

Space engineering

Control engineering

ECSS Secretariat
ESA-ESTEC
Requirements & Standards Division
Noordwijk, The Netherlands

Published by: ESA Publications Division
ESTEC, P.O. Box 299,
2200 AG Noordwijk,
The Netherlands

ISSN: 1028-396X

Price: € 20

Printed in: The Netherlands

Foreword

This Standard is one of the series of ECSS Standards intended to be applied together for the management, engineering and product assurance in space projects and applications. ECSS is a cooperative effort of the European Space Agency, national space agencies and European industry associations for the purpose of developing and maintaining common standards.

Requirements in this Standard are defined in terms of what shall be accomplished, rather than in terms of how to organize and perform the necessary work. This allows existing organizational structures and methods to be applied where they are effective, and for the structures and methods to evolve as necessary without rewriting the standards.

The formulation of this Standard takes into account the existing ISO 9000 family of documents.

This Standard has been prepared by the ECSS-E-60 Working Group, reviewed by the ECSS Engineering Panel and approved by the ECSS Steering Board.

(This page is intentionally left blank)

Introduction

Control engineering, particularly as applied to space systems, is a multi-disciplinary field. The analysis, design and implementation of complex (end-to-end) control systems include aspects of system engineering, electrical and electronic engineering, mechanical engineering, software engineering, communications, ground systems and operations – all of which have dedicated ECSS engineering standards. This Standard is not intended to duplicate them.

This Standard 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 of the discipline where appropriate. For this, and reasons such as the very rapid progress of control component technologies and associated "de facto" standards, this Standard does not go to the level of specifying equipment or interfaces.

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

(This page is intentionally left blank)

Contents

Foreword 3

Introduction 5

1 Scope 9

2 Normative references 11

3 Terms, definitions and abbreviations 13
3.1 Terms and definitions 13
3.2 Abbreviated terms 18

4 Space system control engineering process 19
4.1 General 19
4.2 Definition of the control engineering process 23
4.3 Control engineering tasks per project phase 24

5 Control engineering process requirements 31
5.1 Integration and control 31
5.2 Requirements engineering 33
5.3 Analysis 38
5.4 Design and configuration 44
5.5 Verification and validation 47

Annex A (normative) Control engineering documentation 51
A.1 General 51
A.2 Document requirements list 51
A.3 Document requirements definition 53

Annex B (normative) Control system design report (CSDR) DRD 55

Annex C (normative) Control algorithms specification (CAS) DRD **59**

Annex D (normative) Controlled system analysis report (CSAR) DRD **63**

Annex E (normative) Controlled system verification plan (CSVP) DRD **67**

Annex F (normative) Controlled system verification report (CSVR) DRD **71**

Bibliography **73**

Figures

Figure 1: General control structure 19
Figure 2: Example of controller structure 21
Figure 3: Interaction between CE activities 24

Tables

Table 1: Summary of control engineering tasks 25
Table 2: Control engineering inputs, tasks and outputs, Phase 0/A 26
Table 3: Control engineering inputs, tasks and outputs, Phase B 27
Table 4: Control engineering inputs, tasks and outputs, Phase C/D 28
Table 5: Control engineering inputs, tasks and outputs, Phase E/F 29
Table 6: Contributions of analysis to the CE process 39
Table A-1: Control engineering document requirements list 52

1

Scope

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

The standard covers all aspects of space control engineering including requirements definition, analysis, design, production, verification and validation, transfer, operations and maintenance.

It defines the scope of the space control engineering process and its interfaces with management and product assurance, and explains how they apply to the control engineering process.

When viewed from the perspective of a specific project context, the requirements specified in this Standard should be tailored to match the genuine requirements of a particular profile and circumstances of a project.

NOTE Tailoring is a process by which individual requirements of specifications, standards and related documents are evaluated and made applicable to a specific project, by selection and in some exceptional cases, modifications of existing or addition of new requirements.
[ECSS-M-00-02A, Clause 3]

(This page is intentionally left blank)

2

Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this ECSS Standard. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this ECSS Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references the latest edition of the publication referred to applies.

ECSS-P-001	Glossary of terms
ECSS-E-10 Part 1B	Space engineering — System engineering — Part 1: Requirements and process
ECSS-M-50	Space project management — Information/documentation management

(This page is intentionally left blank)

3

Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ECSS-P-001 and the following apply.

3.1.1
actuator
technical system or device which converts commands from the **controller** into physical effects on the **controlled plant**

3.1.2
autonomy
capability of a system to perform its functions in the absence of certain resources

NOTE The **degree of (control) autonomy** of a space system is defined through the allocation of its overall control functions among **controller** hardware, software, human operations, the space and ground segment, and preparation and execution. A low d**egree of autonomy** is characterized by a few functions performed in the software of the space segment. Conversely, a high d**egree of autonomy** assigns even higher level functions to space software, relieving humans and the ground segment from issuing control commands, at least for the routine operations. The **degree of autonomy** can also be considered to be the amount of machine intelligence installed in the system.

3.1.3
control
function of the controller to derive **control commands** to match the current or future **estimated state** with the **desired state**

NOTE This term is used as in GNC.

3.1.4
control command
output of the **controller** to the **actuators** and the **sensors**

NOTE This definition is applicable in case of **sensors** with command interfaces.

3.1.5
control component

element of the **control system** which is used in part or in total to achieve the **control objectives**

3.1.6
control feedback

input to the **controller** from the **sensors** and the **actuators**

NOTE This definition is applicable to **actuators** with status feedback.

3.1.7
control function

group of related control actions (or activities) contributing to achieving some of the **control objectives**

NOTE A control function describes what the **controller** does, usually by specifying the necessary inputs, boundary conditions, and expected outputs.

3.1.8
control mode

temporary operational configuration of the **control system** implemented through a unique set of **sensors**, **actuators** and **controller** algorithms acting upon a given **plant** configuration

3.1.9
control mode transition

passage or change from one **control mode** to another

3.1.10
control objective

goal that the **controlled system** is supposed to achieve

NOTE Control objectives are issued as requests to the **controller**, to give the **controlled plant** a specified **control performance** 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.

3.1.11
control performance

quantified capabilities of a **controlled system**

NOTE 1 The **control performance** is usually the quantified output of the controlled plant.

NOTE 2 The **control performance** is shaped by the **controller** through **sensors** and **actuators**.

3.1.12
control system

part of a **controlled system** which is designed to give the **controlled plant** the specified **control objectives**

NOTE This includes all relevant functions of **controllers, sensors and actuators**.

3.1.13
controllability

property of a given **plant** to be steered from a given **state** to any other given **state**

NOTE This mainly refers to linear systems, even if it applies also to nonlinear ones.

3.1.14
controlled plant

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

NOTE 1 The control problem is to modify and shape the intrinsic behaviour of the **plant** such that it yields the **control performance** despite its (uncontrolled other) interactions with its **environment**. For space systems, the **controlled plant** can be a launcher rocket, a satellite, a cluster of satellites, a payload pointing system, a robot arm, a rover, a laboratory facility, or any other technical system.

NOTE 2 The **controlled plant** is also referred as the **plant**.

3.1.15
controlled system

control relevant part of a system to achieve the specified **control objectives**

NOTE This includes the **control system** and the controlled **plant**.

3.1.16
controller

control component designed to give the **controlled plant** a specified **control performance**

NOTE The **controller** interacts with the **controlled plant** through **sensors** and **actuators**. 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.

3.1.17
desired state

set of variables or parameters describing the **controller** internal reference for derivation of the **control commands**

NOTE 1 The desired state is typically determined from the **reference state,** e.g. by generation of a profile.

NOTE 2 The difference between desired state and estimated state is typically used for the derivation of the **control commands** (see Figure 2).

3.1.18
disturbance

physical effect affecting the **control performance** that can act onto all components of the **controlled system**

NOTE The source of the disturbance can be internal (if generated inside the **controlled system**) or external (if coming from the **environment**).

3.1.19
environment

set of external physical effects that interact with the **controlled system**

NOTE The environment can act as disturbance on the plant but also on sensors, actuators and the controller.

3.1.20
estimated state
set of variables or parameters describing the **controller** internal knowledge of the **controlled system** and **environment**

3.1.21
estimator
algorithm to determine the current or future **state** (**estimated state**) of a dynamic system from the **measured state**

3.1.22
guidance
function of the **controller** to define the current or future **desired state**

NOTE The term is used as in GNC.

3.1.23
implementation
actual realization of a specific function in terms of algorithms, hardware, software, or human operations

3.1.24
mathematical model
mathematical description of the behaviour of the **plant**, a **control system** component or the **environment**

NOTE This consists of algorithms, formulas and parameters.

3.1.25
measured state
set of variables or parameters derived from physical measurements

NOTE This is based on the **control feedback** of **sensors** and **actuators**

3.1.26
navigation
function of the **controller** to determine the current or future **estimated state** from the **measured state**

NOTE The term is used as in GNC.

3.1.27
observability
property of a given **controlled system** that enables the complete **state** to be determined describing its dynamics

NOTE The observability is normally affected by number and location of sensors.

3.1.28
quantization
process by which **control system** variables are converted into discrete finite units

NOTE This usually applies to **sensor** readings and **control commands** towards **actuators**, and in general, when an analogue-digital conversion is used.

3.1.29
reference state
set of variables or parameters describing the **control objectives** for a **controlled system**

3.1.30
robustness
property of a **controlled system** to achieve the **control objectives** in spite of uncertainties

NOTE 1 The uncertainty can be divided into:

- signal uncertainty, when **disturbances** acting on the **controlled system** are not fully known in advance;
- model uncertainty, when the parameters of the **controlled system** are not well known.

NOTE 2 Robustness is achieved using suitable control algorithms that act against these **disturbances** or are insensitive to **controlled system** parameter variations (e.g. inertia, stiffness).

3.1.31
sensor
device that measures **states** of the **controlled plant** and provides them as feedback inputs to the **controller**

3.1.32
simulation model
implementation of a **mathematical model** in an environment to calculate the behaviour of the model

NOTE It is usually implemented by use of a computer program.

3.1.33
stability
property that defines the specified static and dynamics limits of a system

NOTE A given dynamic system is not fully defined until the notion of stability is precisely mathematically defined according to its characteristics and specified behaviour.

3.1.34
state
set of variables or parameters describing the dynamic behaviour of the **controlled system** at a given time

NOTE 1 The **state** is also referred as state vector.

NOTE 2 The **state** can describe the **true**, **reference**, **desired**, **measured** or **estimated** behaviour (see also Figure 2).

3.1.35
true state
set of variables or parameters defining the actual behaviour of **the controlled system** and **environment**

NOTE 1 The true state is not known.

NOTE 2 In a simulation, the true state is the simulated state of the **sensors**, **actuators**, **plant** and **environment** excluding any measurement error of the **sensors**.

3.2 Abbreviated terms

The following abbreviated terms are defined and used within this document:

Abbreviations	**Meaning**
3D	three-dimensional
A/D	analogue-digital
AOCS	attitude and orbit control system
A&R	automation and robotics
BOL	beginning-of-life
CAD	computer aided design
CAE	computer aided engineering
CAS	control algorithm specification
CE	control engineering
CSAR	controlled system analysis report
CSDR	control system design report
CSVP	controlled system verification plan
CSVR	controlled system verification report
D/A	digital-analogue
DRD	document requirements definition
DRL	document requirements list
EGSE	electrical ground support equipment
EOL	end-of-life
FDIR	failure detection, isolation and recovery
GNC	guidance, navigation and control
H/W	hardware
I/F	interface
ICD	interface control document
LOS	line of sight
MGSE	mechanical ground support equipment
MMI	man-machine interface
PA	product assurance
PDR	preliminary design review
PSD	power spectral density
RMS	root mean square
SEP	system engineering plan
SVF	software verification facility
S/W	software
TBD	to be defined
TM/TC	telemetry-telecommand
TT&C	telemetry, tracking and control
w.r.t.	with respect to
VCD	verification control document
vs.	versus

4

Space system control engineering process

4.1 General

4.1.1 The general control structure

To illustrate and delineate the scope of control engineering, Figure 1 shows a general control structure. This fundamental diagram introduces the following basic concepts and definitions explained below.

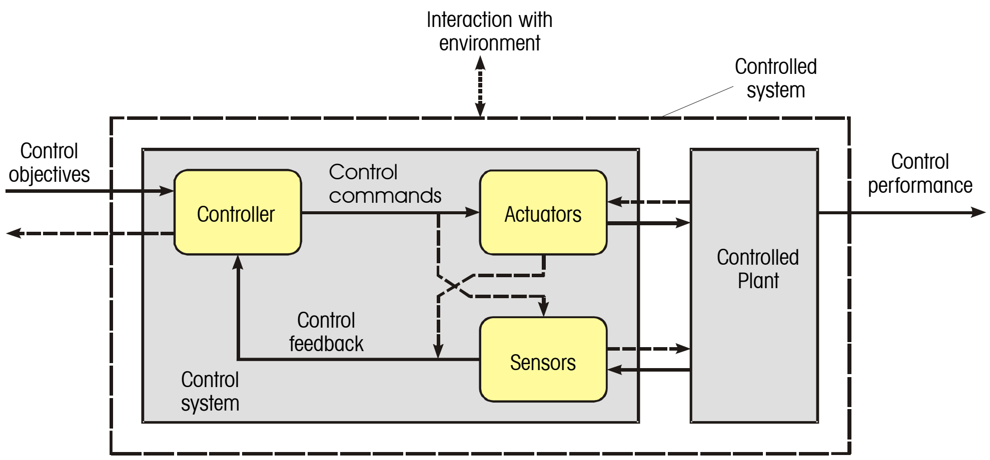

Figure 1: General control structure

The controlled system is defined as the control relevant part of a system to achieve the specified control objectives. It includes the control system (consisting of all relevant functional behaviour of controllers, sensors and actuators) and the controlled plant.

Control engineering always includes some kind of feedback loop. There is a physical system whose intrinsic behaviour and output do not meet the expectations without being modified and shaped (improved in the sense of some well-defined objectives). This is called the controlled plant. For space applications, the controlled plant can be:

- a satellite (e.g. w.r.t. its attitude and orbit, or in the case of active thermal control, w.r.t. to its temperatures) or a cluster of satellites;

- a spacecraft during re-entry and landing, or during rendezvous and docking;
- a pointing system;
- a robot arm system;
- a rover;
- an automated payload or laboratory facility;
- a launcher rocket;
- any other technical system involving control.

The users of the controlled plant have very specific goals. At the most abstract level, they are called control objectives. The purpose is to have a control system that gives the controlled plant a specified control performance, despite its interaction with its environment.

To do this, suitable devices are used: actuators which can convert control commands into physical effects (such as a motor driving a pointing system through a gearbox upon a current command), and sensors which measure states of the controlled plant and provide control feedback to the controller.

Besides this primary flow of information which forms a classical feedback loop, the dashed arrows in Figure 1 also show some secondary flow of information or physical reaction.

With more complex plants, sensors and actuators can be quite complex systems in their own right, with additional cross-coupling of information, e.g. control commands can modify the configuration or parameters of a sensor, or actuators can produce direct feedback to the controller. The dynamics of the controlled plant can have a relevant physical effect on the sensors and actuators, and the operation of the sensors can feed back onto the controlled plant.

Control objectives (as the reference input to the controller) can range from very low level commands (such as set points to a simple servo control loop) to high level mission goals (such as soft landing on the surface of Mars). In the latter case, the actual controller consists of many layers of (usually hierarchically decomposed and refined) control functions and the corresponding sensors, actuators and the controlled plants (which can be suitable abstractions of lower level control loops). In the reverse direction, there can be information (such as status) returned from the controller to a higher level system.

Consequently, the control performance can also range from very elementary behaviour (such as the speed of a motor) to complex high level concepts.

With this in mind, the controller can range from something very confined and simple (such as an analogue on-off logic) to a highly complex system in its own right. In the most general case, the controller is considered to include:

- (digital or analogue electronics) hardware, software and human operation;
- elements in the space segment and in the ground segment (if essential control loops are closed via the ground);
- aspects of planning (quasi "off-line" preparation of the commands to be provided in the future) and of execution of these commands ("on-line" in the sense of the update frequency of the control loop);
- nominal and back-up control (e.g. exception handling, failure detection, and isolation and recovery).

This notion of controller is a general concept which, amongst others, enables a quite natural definition of the various degrees of autonomy or "intelligence" that can be given to a controlled system.

The allocation of control functions to hardware vs. software vs. human operations, space vs. ground, planning vs. execution (which are essentially independent "dimensions" in implementation) for a particular phase (or mode) of a mission are based on a judicious trade-off considering such aspects as predictability of the situation (availability of reliable models), specified reaction time, available on-board computer resources, available telecommunications coverage and bandwidth, decision-making complexity, cost of development and operations, and acceptable risk.

The consideration of human operations and ground systems in the control engineering process is not surprising, since, after all, they serve essential roles in achieving a control performance and thus are part of a higher level controller. In any case, for all specific aspects of ground systems and operations this Standard refers to ECSS-E-70 Part 1 and ECSS-E-70 Part 2.

In the sense of classical control theory, the controller has an internal functional structure with the following functions (as shown in Figure 2):

- determination of current or future desired state;
- determination of current or future estimated state;
- derivation of control commands.

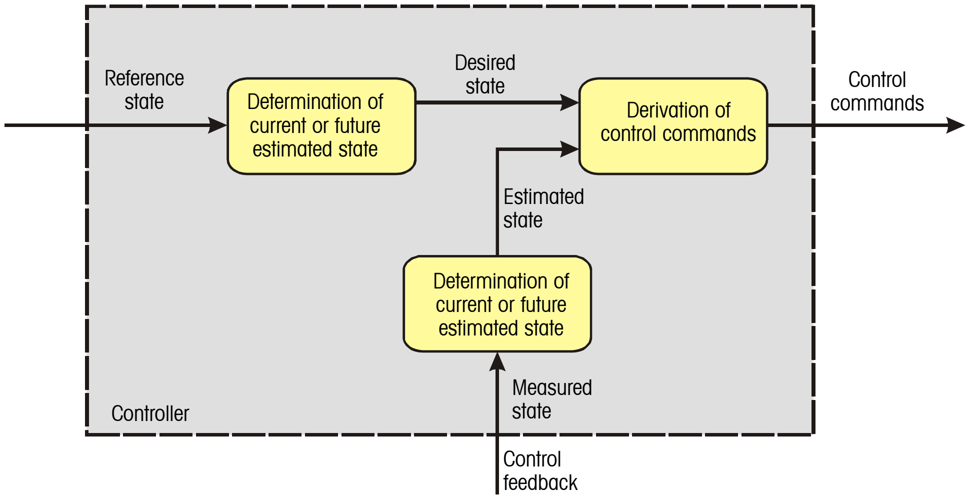

Figure 2: Example of controller structure

This functional concept can be applied to very simple controllers in which some of the functions can be absent (e.g. when the desired state is identical to the reference state) but also for more complex controllers for which the determination of current or future desired state includes the computation of a whole trajectory (e.g. a launcher trajectory).

NOTE For GNC systems the three controller functions shown in Figure 2 correspond to the classical GNC functions:

- determination of desired state ⇔ guidance function;
- determination of estimated state ⇔ navigation function;
- derivation of control commands ⇔ control function.

Besides these "classical" controller functions the controller can, of course, include a whole set of other functions, e.g. for switching control modes (controller internal and for sensors and actuators), monitoring of control system and plant status, updating of models, failure detection, isolation and recovery which are not shown in Figure 2.

4.1.2 Control engineering activities

From the general control structure introduced above, it becomes clear that control engineering includes, as a minimum:

- analysis of the mission objectives in order to define the control objectives;

- analysis and modelling of the controlled plant and its interaction with the environment;
- analysis, modelling and specification of sensors and actuators (configuration and characteristics) w.r.t. the control requirements;
- requirements analysis and specification, design and configuration of the controller;
- verification of the control performance;
- control system related ground operations.

Consequently control engineering:

- is multi-disciplinary (which cannot be performed without significant insight into at least mechanics, dynamics, the space environment and its effects, digital and analogue electronics, control theory, computer systems and networks, software engineering, and operations);
- has a strong system aspect and therefore a significant level of interaction with the system engineering process specified in ECSS-E-10 Part 1.

4.1.3 Organization of this Standard

This Standard is organized as follows:

- This Clause 4 sets the framework for the control engineering process. The main engineering activities are defined and characterized by their inputs, the tasks to be performed, outputs (including documents), milestones, and relationship to the project phases.
- Clause 5 treats each of these engineering activities in detail, specifying the requirements for tasks and expected outputs in detail. These are the core normative requirements for control engineering in space systems.
- Annex A gives a list of the key documents to be produced in the control engineering process.
- Annexes B to F describe the structure and content of the key documents listed in Annex A, one by one.

4.1.4 Relationship with other standards

4.1.4.1 General

The following paragraphs discuss how this Standard interfaces with other ECSS standards and points out relations to non-ECSS standards.

4.1.4.2 ECSS engineering standards

- ECSS-E-00 defines the engineering domain and the system engineering process. The engineering functions, as one of the dimensions of the engineering domain, serve as the basic structuring principle also of this Standard.
- ECSS-E-10 Part 1 “System engineering” defines requirements for space system engineering. Because of the significant system aspect of control engineering, ECSS-E-10 Part 1 and this Standard have a high level of interaction.
- Because of the multi-disciplinary character of control engineering, this Standard has been developed in a harmonized way with all the parallel Level 2 engineering standards for the disciplines of electrical and electronic engineering (ECSS-E-20), mechanical engineering (ECSS-E-30 Part 1 to Part 8), software engineering (ECSS-E-40 Part 1), communications (ECSS-E-50 Part 1), and ground systems and operations (ECSS-E-70 Part 1). Where control specific issues are concerned, however, this Standard has a higher level of precedence.

4.1.4.3 ECSS project management standards

The ECSS M series of standards define the requirements applicable to the management of space projects. Of particular relevance are:

- ECSS-M-30 which defines the sequence of the engineering functions w.r.t. the different project phases;
- ECSS-M-40 which specifies the relationship between project phases, reviews, end product states, associated documents and configuration status.

4.1.4.4 ECSS product assurance standards

The ECSS Q series of standards define the requirements applicable to product assurance of space projects. The system engineering product assurance requirements are applicable to control engineering.

4.2 Definition of the control engineering process

The control engineering process (CE process) is itself a part of the system engineering process as defined in ECSS-E-10 Part 1. As such it can also be broken down into the same engineering activities:

- **Integration and control**, which ensures the integration of the various control related disciplines throughout all project phases towards the total definition and realization of the controlled system**.**
- **Requirements engineering**, which includes proper interpretation of the mission and system requirements, coherent and appropriate derivation of control requirements, definition of lower component or equipment level requirements and continuous supervision of their status and traceability.
- **Analysis**, performed at all levels and in all domains for the purpose of resolving control related functional and performance requirements, evaluating control design alternatives; consolidating and verifying control performances and complementing tests.
- **Design and configuration**, which includes the derivation of a physical control architecture and the controller design capable of meeting the control requirements (supported by proper analyses and trade-offs). Design also includes the derivation of all the control budgets with appropriate budget methodology and margin policy.
- **Verification and validation**, to demonstrate, through a dedicated process, that the controlled system meets its control objectives and requirements.

These different control engineering activities are, at various phases of the system development, conducted in parallel to support one another in the proper development of the control system and of its components. These interactions are shown in Figure 3.

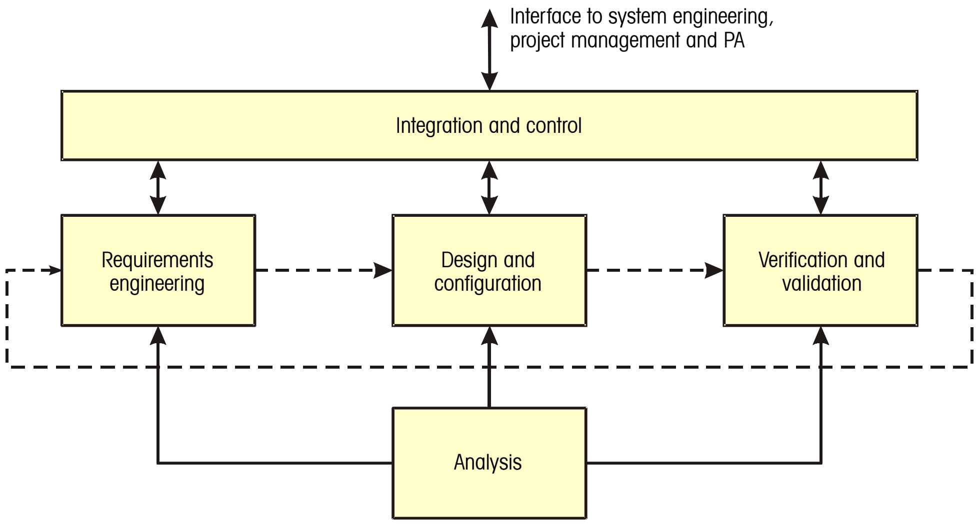

Figure 3: Interaction between CE activities

Table 1 provides a summary of the specific control engineering tasks corresponding to each activity.

After the functional specification of the control system, it is likely that hardware, software and operations support items are designed and developed (or procured) along parallel paths or branches within the control engineering process by corresponding disciplines. Consequently, the control engineering process is:

- iterative between system engineering and lower assembly or equipment level engineering. The control engineering process is defined so as to make these iterations feasible;
- progressive from preliminary design to verification and in-flight validation. The usual control engineering tasks, inputs and outputs according to the chronological phases of a programme are detailed in subclause 4.3;
- particularly iterative between requirements engineering, design-configuration, verification-validation and analysis.

4.3 Control engineering tasks per project phase

This subclause provides details of the engineering tasks to be performed at each phase of the project. Tables 2 to 5 show the inputs, the tasks and the outputs for each activity.

Table 1: Summary of control engineering tasks

Control engineering activity	Specific control engineering tasks
Integration and control	– Organization and planning of control engineering activities. – Contribution to system engineering database. – 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. – Support to change management involving control (including in‐flight maintenance). – Control engineering capability assessment and resource management.
Requirements engineering	– Generation of control requirements from system and mission requirements. – Contribution to system requirements to meet control requirements. – Allocation of control requirements to sub‐assemblies or equipment (sensors, actuators and controller H/W). – Definition of control S/W requirements. – Definition of control interface requirements between control components. – Definition of control operations requirements. – Definition of control verification requirements.
Analysis	– Selection of adequate analysis tools and methodologies. – Requirements evaluation and budgets breakdown. – Disturbances evaluation. – Numerical trade studies to support the definition of the control architecture with respect to requirements considering programme imposed constraints such as cost, schedule and risk. – Numerical analysis to support the control design. – Performance verification analysis (including simulation). – Numerical analysis to support in‐flight evaluation.
Design and configuration	– Definition of functional control architecture (including functional interfaces). – Definition of operational control architecture (modes). – Definition of physical control architecture (H/W, S/W and human operation). – Design of control concepts and algorithms. – Control design trade‐offs. – Generation of control budgets. – Contribution to selection and procurement of control components. – Contribution to system configuration management.
Verification and validation	– Definition of control verification and validation strategy (including specification of requirements for test environments). – Definition of control verification and validation strategy. – Preliminary verification of performance by analysis or prototyping. – Final functional and performance verification by analysis. – Final verification and validation of controlled system (H/W, S/W and human operation) by hardware‐in‐the‐loop tests. – In‐flight validation of controlled system behaviour.

Table 2: Control engineering inputs, tasks and outputs, Phase 0/A

0/A	Integration and control	Requirements engineering	Analysis	Design and configuration	Verification and validation
Inputs	– System development schedule – System development approach and constraints	– System objectives – Mission requirements – System performance requirements	– Controlled system objectives – Preliminary control system requirements	– Control system design concepts of similar space systems	– System verification and validation approach
Tasks	– First assessment of control system development cost and schedule – Generation of inputs to the 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 – Control system life cycle definition	– Analysis of control requirements feasibility for control system alternatives – Preliminary disturbances evaluation – Preliminary performance assessment – Initial sensitivity analysis – Identification of control system critical aspects	– Establishment and trade-off of control system design concepts – Establishment of control system design baseline (including preliminary FDIR concept)	– Control engineering support for definition of verification and validation concepts – Preliminary definition of control verification and validation methods and strategies
Outputs	– Inputs to project and system engineering plan – Inputs to cost estimates and schedule estimates – Inputs to technology development plan	– Inputs to system requirements documentation	– Control system analyses	– Preliminary control system design and analysis report	– Inputs to development and verification planning

Table 3: Control engineering inputs, tasks and outputs, Phase B

B	Integration and control	Requirements engineering	Analysis	Design and configuration	Verification and validation
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 analyses	- Phase 0/A control design	- System verification plan - Phase 0/A control verification plan
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 - Controlled system sensitivity 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) - Preliminary definition of control related FDIR - Selection of control components and technologies - Establishment of control related budgets and margins	- Prepare controlled system verification plan - Provide inputs to lower level verification plans - Provide inputs to the management plan - Support Phase C/D verification planning
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 - Inputs to requirements database - Inputs to interface control documents	- Controlled system analysis report (including simulation models description)	- Control system design report (incl. design justification) - Preliminary control algorithms specification - Preliminary control system budgets	- Controlled system verification plan - Preliminary controlled system verification report

Table 4: Control engineering inputs, tasks and outputs, Phase C/D

C/D	Integration and control	Requirements engineering	Analysis	Design and configuration	Verification and validation
Inputs	– Phase B project planning and cost estimates – Control life cycle Phase B	– 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 controlled system verification plan
Tasks	– Support of system engineering and project management (including risk management) – Management of required control system changes – Support of operations – Review of data packages – Support to Phase E/F planning and cost estimate	– Update of specifications – Review and assessment of control requirements changes – Review and assessment of system changes related to control	– Detailed controlled system performance analysis – Update of sensitivity 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 – Detailed design of control-related FDIR – Review of control budget and margins analysis	– 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
Outputs	– Updated inputs to project and system engineering plan – Inputs to system database – Inputs to operations handbook or user manual – 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) – Final control system budgets	– Controlled system verification report – Inputs to in-flight verification plan

Table 5: Control engineering inputs, tasks and outputs, Phase E/F

E/F	Integration and control	Requirements engineering	Analysis	Design and configuration	Verification and validation
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	- In-flight verification plan
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)	- Support controlled system operational performance verification - Support system review
Outputs	- Inputs to disposal plan	- New control related operational requirements	- Inputs to controlled system operational performance report - Updated control controlled system analysis report - Inputs to payload data evaluation	- Controller design updates (updated control system design report)	- Inputs to in-flight acceptance report - Inputs to periodic mission reports

(This page is intentionally left blank)

5

Control engineering process requirements

5.1 Integration and control

5.1.1 General

5.1.1.1
The integration and control activities contribute to system engineering from a control engineering point of view and support the system engineering management activities.

5.1.1.2
Integration and control shall be consistent with the system engineering plan (SEP) and system engineering integration and control requirements in subclause 4.3 of ECSS-E-10 Part 1B.

5.1.2 Organization and planning of CE activities

5.1.2.1
Control engineering shall contribute to the system engineering management plan to define, organize and plan all control engineering activities to achieve the specified control performance.

NOTE This applies especially to the control development and verification logic which is closely related to the system design and development planning.

5.1.2.2
Control engineering shall contribute to and participate in all major project reviews to assess the system design and system design changes from control point of view.

5.1.3 Contribution to system engineering data base and documentation

5.1.3.1
Control engineering shall provide inputs to the system engineering database concerning controller data.

5.1.3.2
Control engineering shall provide inputs to the system engineering database w.r.t. control related sensor and actuator parameters (e.g. flight dynamics database).

5.1.3.3

Control engineering shall provide a consistent set of control related documentation for the complete development process which is in line with the general system documentation.

NOTE For the content and format of the control related documentation, see DRDs in Annex A to Annex F.

5.1.4 Management of interfaces with other disciplines

5.1.4.1

Control engineering shall provide inputs and review related system parameters, constraints and interfaces, including at least:

a. electrical interfaces (e. g. noise, quantization, sampling and timing);

b. mechanical interfaces (e.g. mass properties, alignment, stiffness, eigenfrequencies and micro-vibrations);

c. thermal interfaces;

d. software interfaces (control functions realized by S/W);

e. ground segment interfaces;

f. operational interfaces;

g. TT&C;

h. optical.

5.1.4.2

Control engineering shall ensure that the control related system parameters, constraints and interfaces are endorsed and approved at system level.

5.1.5 Contribution to human factors engineering

a. Control engineering shall contribute to human factors engineering in the case when humans are part of the control loop.

b. The following factors shall be considered:

   1. human performance capabilities;

   2. human-machine interfaces;

   3. training of control operators.

5.1.6 Budget and margin philosophy for control

a. For control related budgets with several contributors, summation rules shall be defined and used consistently throughout the design process.

b. A margin policy shall be established and applied.

   NOTE Budget methodology and margin philosophy can evolve during the development according to the level of maturity of the control system.

5.1.7 Assessment of control technology and cost effectiveness

5.1.7.1

a. The programmatic risk w.r.t. the maturity of the control related technology shall be analysed and assessed.

b. The analysis and assessment referred in a. shall be done for the

   1. controller (e.g. H/W – S/W – human and analogue-digital), and

   2. sensors and actuators.

5.1.7.2
The effort (cost and risk) for the verifications of the control objectives and requirements shall be assessed.

5.1.8 Risk management

Control engineering shall contribute to risk analysis from a technical point of view.

5.1.9 Support to control components procurement

5.1.9.1
Control engineering shall support system engineering for the procurement of the controller H/W and S/W.

5.1.9.2
Control engineering shall support system engineering for the procurement of sensors and actuators.

5.1.10 Support to change management involving control

5.1.10.1
Control engineering shall support the management of nonconformances related to control.

5.1.10.2
Control engineering shall handle changes related to controller design and implementation.

5.1.10.3
Control engineering shall review changes in control related disciplines.

5.1.11 Control engineering capability assessment and resource management

5.1.11.1
Control engineering shall assess the control related capability and experience.

5.1.11.2
Control engineering shall perform the related resource management w.r.t.

a. human resources, and

b. tools.

5.2 Requirements engineering

5.2.1 General

Control requirements, addressed by control engineering, can be of two types:

- Requirements to be met by the controlled system. These requirements are derived from system level objectives and encompass:
  - requirements applying to the controller,
  - requirements applying to sensors and actuators, and
  - requirements applying to the plant (e.g. free field of view or inertia balancing).

  The requirements can originate from the specified control objectives or from other constraints (e.g. controlled system verification).
- Requirements or constraints the controlled system puts on ground operations, in particular ground processing requirements.

5.2.2 Generation of control requirements

5.2.2.1

The control requirements shall be derived from the directly applicable system requirements.

5.2.2.2

Control requirements engineering shall consider constraints imposed by other system requirements (e.g. electrical power, mechanical configuration, thermal conditions and operations).

5.2.2.3

a. The control requirements shall be allocated to lower level requirements for the control components (controller, sensors and actuators).

b. The allocation referred in a. shall be supported by

   1. analyses (budget oriented and simulation), and
   2. tests (e.g. on existing equipment or breadboards).

   NOTE The allocation of lower level requirements is usually an iterative process.

5.2.2.4

Control requirements engineering shall maintain traceability and justification of the control requirements, in line with the system requirements engineering process.

NOTE Beside the top-down requirements engineering, the writing of control requirements can also take into account the bottom-up flow of requirements stemming from the reuse of, for example, existing equipment and control law elements.

5.2.2.5

Control requirements engineering shall take into account system FDIR requirements and failure management definitions.

5.2.2.6

Control requirements engineering shall support system requirements engineering to identify and eventually resolve conflicts between requirements, requirements ambiguities and conflicts between requirements and environmental factors or design constraints.

5.2.2.7

Through an appropriate document (e.g. ICD), control engineering shall define and justify any control requirement generating a specific system constraint (e.g. minimum allowable thruster tilt for plume effect limitation, sensors-actuators implementation w.r.t. FOV, alignment, mechanical stiffness, eigenfrequencies).

5.2.3 Allocation of control requirements to control components

5.2.3.1 General

Subclauses 5.2.3.2 to 5.2.3.5 specify the requirements to be identified and defined by control engineering for any control component.

NOTE The level of detail depends on the phase of the project.

5.2.3.2 Sensors

a. As a minimum, the following sensor properties shall be defined as part of the control system design:

1. Functional and performance requirements.

EXAMPLE Usual functional and performance requirements are:

- 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 A/D conversion (RMS, PSD);
- FDIR requirements.

2. Operational requirements.

EXAMPLE Operational requirements are:

- measurement modes (e.g. fine mode or coarse mode);
- conditions for mode transitions;
- operational restrictions (e.g. Sun exclusion angle for an optical sensor and recovery after blinding);
- calibration requirements: type (permanent or occasional), frequency, duration and parameters to refresh.

NOTE The functional and performance parameters under 5.2.3.2.a.1. can be specified separately for the different modes.

3. Configuration requirements.

EXAMPLE Configuration requirements are:

- accommodation requirements (e.g. free field of view, and minimum stiffness between actuators and sensors);
- disturbance constraints from internal sources (e.g. vibrations).

4. Interface requirements.

EXAMPLE Interface requirements are:

- alignment requirements (bias and stability);
- electrical interface requirement (e.g. maximum noise for analogue interfaces);
- data interface requirement (e.g. resolution).

5. Verification requirements.

EXAMPLE Verification requirements are:

- test interface requirements (stimuli inputs);
- special provisions for ground testing.

b. All properties of the sensors should be checked for feasibility.

5.2.3.3 Actuators

a. As a minimum, the following actuator properties shall be defined as part of the control system design:

1. Functional and performance requirements.

EXAMPLE Functional and performance requirements are:

- actuation principle;
- absolute-relative accuracy (before-after calibration);
- operating range (including limitations by operating conditions);
- resolution;
- linearity;
- maximum allowed unpredictable bias;
- actuation bandwidth, 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 D/A conversion (RMS, PSD);
- FDIR requirements.

2. Operational requirements.

EXAMPLE Operational requirements are:

- actuation mode (e.g. torque or speed control), conditions for mode transitions;
- operational restrictions (e.g. maximum number of actuations);
- calibration requirements: type (permanent or occasional), frequency, duration and parameters to refresh.

NOTE The functional and performance parameters under 5.2.3.3.a.1. can be specified separately for the different modes.

3. Configuration requirements.

EXAMPLE Configuration requirements are:

- accommodation requirements (e.g. position and orientation of actuator);
- avoidance of disturbances caused by actuator.

4. Interface requirements.

EXAMPLE Interface requirements are:

- alignment requirements (bias and stability);
- electrical interface requirement (e.g. maximum noise for analogue interfaces);
- data interface requirement (e.g. resolution).

5. Verification requirements.

EXAMPLE Verification requirements are:

- testing interface requirements (stimuli outputs);
- special provisions for ground testing.

b. All properties of the actuators should be checked for feasibility.

5.2.3.4 Controller hardware requirements

a. The following requirements for the controller hardware shall be defined:

1. sampling rates for sensor reading;
2. sampling rates for actuator commanding;
3. sampling rates for controller functions;
4. allowed processing delays for reading sensor information, controller processing and actuator commanding;
5. allowed time jitter in delays;
6. electrical interface requirements (including requirements for anti-aliasing filters);
7. requirements on computational performance and memory size.

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

b. All properties of the controller hardware should be checked for feasibility.

5.2.3.5 Controller software requirements

a. The following requirements for the controller software shall be defined:

1. Control engineering shall define the algorithms for all “classical” control functions (see Figure 2) to be implemented in the controller:
   (a) definition of desired state;
   (b) determination of estimated state;
   (c) derivation of control commands.
2. Control engineering shall define the algorithms for all other control functions, as a minimum for
   (a) control mode management,
   (b) control system status monitoring, and
   (c) failure detection, isolation and recovery.
3. Control engineering shall specify the precision for the calculation of the control algorithms.
4. Control engineering shall define the control software timing conditions (sampling rates, delays and jitter) in a consistent way together with the controller hardware timing conditions.
5. Control engineering shall define the requirements for safety critical control functions.
6. Control engineering shall identify and define the control S/W interface requirements,
   (a) from-to sensors and actuators, and
   (b) from-to system level control (on-board or ground).

b. All properties of the controller software should be checked for feasibility.

5.2.4 Control verification requirements

Control engineering shall identify and define the control verification requirements (e.g. test interfaces) enabling the verification process at all levels (component to system level).

5.2.5 Control operations requirements

a. Control engineering shall specify the modes and mode transitions.

b. For each mode, control engineering shall define how the control functions shall be allocated, e.g. control between hardware-software-human operations, and between on-board and on-ground.

c. Control engineering shall define the control operator interface requirements (e.g. specified MMI functions and processing requirements).

d. Control engineering shall define the telemetry data needs from control point of view.

e. Control engineering shall define the calibration process and the ground software requirements.

f. Control engineering shall define how the ground system manages failures of the control system in a manner that is consistent with the overall system failure management.

5.3 Analysis

5.3.1 General

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

1. supporting the allocation of requirements among the different control functions;
2. substantiating the selection of control functional or physical architectures and implementations;
3. trading off alternative control solutions;
4. identifying design risk factors;
5. verifying the controlled system performance relative to its requirements and within the applicable environment.

NOTE 1 In particular, analysis contributes to the whole control engineering process, as depicted in Figure 3.

NOTE 2 In line with ECSS-E-10 Part 1, the analysis process interacts strongly with all the other control engineering activities.

b. Within control engineering the objects of the analysis shall be the controller, the sensors and actuators, the controlled plant, and the external environment (see Figure 1).

NOTE These elements are analysed in order to assess the capability of the controlled system to map the control objectives into the control performance.

5.3.2 Analysis tasks, methods and tools

5.3.2.1

For all control engineering functions, analytical methods and tools shall be used and properly adopted to each analysis task (per project phase).

NOTE A list of usual analysis methods and tools is summarized in Table 6.

Table 6: Contributions of analysis to the CE process

Control engineering activity	Analysis tasks	Usual methods and tools
Requirements engineering	– requirement analysis – requirements feasibility assessment – disturbance quantification – error source identification and relevant numerical figures allocation to budgets	– analytical relationships and models – spreadsheet analysis tools – control CAE tools – control, environment, sensors, actuators and plant models
Design	– numerical trade studies in support of control architecture definition – numerical analysis to support control design – disturbance effects detailed analysis – stability – robustness – sensitivity to additional or parametric disturbances – performance against applicable requirements – control budget numerical figures consolidation	– analytical relationships and models – spreadsheet analysis tools – 3D CAD system model – control CAE tools – closed-loop simulation (including detailed control, environment, sensors, actuators and plant models) – simulation data analysis tools (e.g. statistical methods) – time-frequency domain methods – linear and non-linear methods
Verification	– performance analysis – test data analysis resulting from H/W-, S/W-, human-in-the-loop tests – in-flight data analysis – support to payload data evaluation	– closed-loop simulation (including detailed control, environment, sensors, actuators and plant models) – test data evaluation tools (e.g. statistical methods) – telemetry data processing tools – control CAE tools

5.3.2.2

Depending on the specific control engineering process phase, one or more analysis methods shall be selected (or combined).

NOTE Examples of usual approaches to analysis are:

- top-down;
- multi-layered, hierarchical;
- simplified, conceptual;
- analytical, equation based;
- numerical computer simulation based;
- hardware-in-the-loop and software-in-the-loop tests.

5.3.2.3

a. Analysis shall be based on validated methods and tools.

b. The adequacy of the tools for the analysis of the control system shall be demonstrated.

c. If, in the case of new tool development, control engineering contributes to the specification, development and validation of such tool, this activity shall be managed as part of the control engineering process.

5.3.2.4
The selected tools shall be identified and documented in terms of

a. type of tool,
b. version,
c. implemented methods, and
d. platform (H/W and operating system).

5.3.2.5
One or a combination of the following categories of generic methods and tools shall be used to develop models:

a. spreadsheet based tools;
b. computer aided engineering tools (CAE), e.g. mathematical (analytical, numerical, symbolical) control design and simulation tools;
c. multi-body dynamic modelling and simulation tools;
d. environment simulation tools;
e. functional modelling tools;
f. auxiliary tools for model parameter generation (pre-processing);
g. kinematic analysis tools;
h. trajectory analysis tools.

5.3.2.6
Control analysis and simulation tools supporting compatibility for data exchange with tools used by other engineering domains should be used.

5.3.2.7
Control analysis and simulation tools which are portable across different platforms should be used.

5.3.3 Requirements analysis

5.3.3.1
In the framework of the requirements engineering process outlined in subclause 5.2, analysis is extensively used to support (as a hierarchical flow):

- decomposition of high level mission objectives (customer needs) into feasible control objectives;
- definition of numerical requirements for the controlled system;
- apportionment of requirements for the controlled system to lower level requirements for the different control components (controller, sensors and actuators) and the plant as referenced in Figure 1;
- definition of human-in-the-loop constraints.

5.3.3.2
For each phase defined in Table 2 to Table 5, requirements analysis shall result in a detailed control error budget to be used as input for the technical specification of control components.

5.3.3.3
Analysis shall support the optimization of control error budget allocation via trade-off studies, market survey and risk analyses (e.g. considering the maturity levels of the new technologies w.r.t available technologies).

5.3.3.4

Analysis shall assess feasibility of requirements allocated to the different control components.

NOTE For guidelines on requirements allocation analysis for positioning and pointing systems, see ESA‐NCR‐502 (ESA Pointing Error Handbook).

5.3.4 Disturbance analysis

5.3.4.1

Control engineering shall perform the analysis to define the internal and external disturbances to the controlled system as defined in Figure 1.

5.3.4.2

Disturbances originating in the plant shall be defined based on the system requirements.

5.3.4.3

a. External disturbances due to the space environment shall be defined.

NOTE For space environment, see ECSS‐E‐10‐04.

b. Usage of different models (e.g. for special applications analysis) shall be

1. justified, and
2. agreed with the customer on a case-by-case basis.

5.3.4.4

Internal disturbances (e.g. actuator vibration, friction, and noise) shall be modelled using verified parameters (e.g. manufacturer data) or parameters identified by dedicated tests.

NOTE Worst case parameters can be used to avoid tests provided that robustness is demonstrated w.r.t these parameters.

5.3.4.5

Disturbance analysis shall cover all mission scenarios.

5.3.4.6

Disturbance analysis shall cover the whole mission lifetime of the controlled system.

5.3.5 Performance analysis

5.3.5.1

a. The performance analysis shall assess that the controlled system performance is coherent with

1. the control objectives generated by the requirement engineering process, and
2. the numerical requirements defined by the requirements analysis.

b. Performance analysis shall be conducted during all the phases of the control development process.

5.3.5.2

For performance analysis, mathematical models shall be developed and used.

NOTE The number and detail of the models depend on the project phase.

5.3.5.3

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

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

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

5.3.5.4

During Phase C/D, a detailed closed-loop simulation model (i.e. including environment, plant, sensors, actuators and controller) shall be developed with the aim of performing the control system design optimization and the controlled system verification processes.

5.3.5.5

a. The mathematical models used for detailed simulations of the controlled system shall include:

   1. Model of the controlled plant:
      (a) dynamics,
      (b) kinematics (coordinate transformations).
   2. Models of the sensors.
   3. Models of the actuators.
   4. Model of the controller hardware:
      (a) timing conditions,
      (b) A/D and D/A quantization.
   5. Model of the controller functions (controller software):
      (a) control algorithms (as defined in subclause 5.2.3.4) with representative timing and numerical precision control algorithms;
      (b) interface to system level control.

      NOTE For example, for
      - reference signals (reference state), and
      - mode switching commands.
   6. Model of the relevant disturbance sources:
      (a) internal disturbance sources (within the controlled system), which can be part of the sensor, actuator, controller or plant models;
      (b) external disturbance sources (from the environment), which can be part of the sensor, actuator, controller or plant models.
   7. Model of the environment (for modelling the control relevant influences onto the controlled system):
      (a) nominal inputs (e.g. Sun position as input to sun sensor),
      (b) external disturbances sources.
   8. Model of the control signals interfaces.

      NOTE For example, for
      - timing conditions, and
      - noise (for analogue interfaces).

b. The models defined in a. above shall be calculated with a numerical precision in line with the control problem.

NOTE The timing of a complex signal interface (e.g. bus interface with protocol) can be modelled separately and cannot simply be allocated to one control component. The timing conditions for such an interface can be additionally influenced by other effects (e.g. bus load caused by other equipment).

5.3.5.6

The mathematical model shall provide all outputs for assessing the controlled system performance by means of

a. direct evaluation of the outputs in the time domain, and

b. input-output data post-processing.

5.3.5.7

Mathematical model simulations shall be used to support the design activity for the following tasks:

a. assessment of fulfilment of control objectives;

b. sensitivity analyses for design trade-offs and optimization of product selection;

c. sensitivity analyses for assessment of control design robustness (against variations and uncertainties in the controlled system parameters).

5.3.5.8

In the framework of the final performance verification, performance analysis based on the mathematical model shall assess, for the mission operating scenarios, the controlled system requirements fulfilment in terms of:

a. time domain requirements such as:

1. response to reference signals (e.g. response time, settling time, and tracking error for command profiles);
2. accuracy and stability errors in the presence of disturbances;
3. measurement errors (e.g. attitude knowledge).

b. frequency domain requirements (e.g. bandwidth).

5.3.5.9

The performance analysis shall take into account all control modes (nominal and back-up modes).

5.3.5.10

Performance analysis based on detailed mathematical model simulation shall support the system in-flight performance evaluation, including the identification and solution of in-flight control system failures.

5.3.5.11

a. Control related budgets (e.g. error budget) shall be established, maintained and compared to the control requirements.

b. The performance analysis shall support the maintenance of control budgets throughout the control engineering process.

c. The value used for each contributor shall be justified by analysis or measurement (ground or flight).

5.4 Design and configuration

5.4.1 General

The control design engineering process consists of the following steps:

- Design of the functional and operational architecture of the control system, including its control concept(s) and interfaces with the controlled plant. This can be supported by analysis, simulation or by preliminary physical implementation (prototyping).
- Allocation of the control functions to control hardware, control software and human operations (including allocation between ground and on-board functions), both for preparation and utilization, according to the operational requirements.
- Detailed design of the control system physical architecture, defining the implementation of all functions in hardware and software.

The above steps are, in principle, executed sequentially but

- sometimes an iterative process is used, and
- parts of these steps are omitted in case of system constraints (e.g. re-use of existing design or implementation).

Control design is also performed iteratively with analysis and verification.

During the preliminary design phase, the concept and architecture selections are supported by trade-offs to enable performance, cost, schedule and risk optimization.

5.4.2 Functional design

5.4.2.1

The functional design process, also called “functional analysis”, consists of a resolution of control objectives into control system functions. This is usually achieved through a top-down process.

5.4.2.2

a. Control engineering shall define a functional design consisting of the control system functions (and sub-functions) to meet the control objectives.

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

c. The functional design shall be compatible with the system functional analysis.

5.4.3 Operational design

5.4.3.1

The logical organization of the functions leads to a logical or operational architecture made up of a set of control modes and transitions between these modes.

5.4.3.2

Control engineering shall define the operational control architecture, which consists of a set of control modes and transitions between modes covering all specified (nominal and non-nominal) conditions of operations of the control system.

NOTE The composition of functions and allocations to a control mode can be expected to be based on certain existing and common knowledge (experience) of optimum use of sensors, actuators, controllers and operational items.

5.4.3.3

The operational control architecture should be presented in the form of diagrams showing control mode transitions and data flows.

5.4.3.4

For each control mode, the design shall identify

a. the functions involved,

b. the allocation of functions to H/W, S/W and humans,

c. the allocation of functions to ground and on-board,

d. the conditions of validity of the control mode, and

e. its contribution to the control objectives.

5.4.3.5

a. The design shall identify the conditions for transitions between modes:

   1. starting conditions (previous mode and specific conditions);

   2. when the transition occurs (trigger conditions);

   3. end-conditions (subsequent mode and specific conditions).

b. The functions to be performed during the transitions shall be described.

5.4.3.6

Control engineering shall check that the operational and functional design covers all the control objectives.

5.4.4 Control implementation architecture

5.4.4.1

The physical control architecture is the assembly of components (sensors, actuators, controller and plant realized by hardware, software or humans) that are used to meet the control objectives. In the design of the control system, control engineering takes into account the limitations of these physical elements to achieve a feasible design. It also uses the physical characteristics of these elements to design the controller. These activities often interact with other disciplines and for complex systems are expected to be performed in coordination with system engineering.

5.4.4.2

Control engineering shall define a set of requirements for sensors which can meet all the control objectives in terms of performance, redundancy, observability and operability.

5.4.4.3

Control engineering shall

a. contribute to the definition of a sensor configuration (sensor product and accommodation);

b. verify that the selected sensor configuration is compatible with the control system design.

5.4.4.4

Control engineering shall define a set of actuators which can meet all the control objectives in terms of controllability, performances and redundancy.

5.4.4.5

Control engineering shall:

a. contribute to the definition of an actuator configuration (actuator product and accommodation);

b. verify that the actuator configuration selected is compatible with the control system design.

5.4.4.6

Control engineering shall check if the operational dynamic conditions of plant are compatible with the selected configuration of sensors and actuators.

5.4.4.7

Control engineering shall:

a. contribute to the design of the plant with respect to the system dynamics and kinematics affecting the control performance;

b. verify that the selected plant physical configuration is compatible with the control system design.

5.4.4.8

Control engineering shall contribute to the design of the electrical system architecture w.r.t. electrical interfaces affecting the control performance.

5.4.4.9

Control engineering shall contribute to the on-board processing architecture w.r.t processing capability, data rates, inputs-outputs, memory affecting the control performance.

5.4.4.10

Control engineering shall verify that the control design is compatible with the predicted failure or evolution of the physical characteristics of the control components (BOL and EOL), in particular due to environment conditions.

5.4.4.11

Control engineering shall verify that the definition of interfaces with ground facilities, humans and with other space vehicles, if they are part of the system, enables the control objectives to be achieved.

5.4.5 Controller design

5.4.5.1

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 algorithms are designed to achieve the control objectives while being robust to uncertainties or predicted evolutions in the controlled system (controlled plant or control components). Furthermore, the controller can include algorithms that are designed to react to possible (expected) failures in the control system components or the plant.

The control algorithms can be implemented in digital or analogue form.

5.4.5.2

a. The controller shall be designed such that the controlled system meets the specified performance requirements.

b. The effects influencing the control loop (such as performance of the control components, dynamic behaviour of the plant, and disturbances due the environment) should be taken into account in the controller design.

NOTE The performance requirements of the controlled system depend on all these effects.

5.4.5.3
The controller design shall be robust against uncertainties or predicted evolutions.

NOTE These evolutions can be due to:

- changes in the physical variations of hardware parameters between BOL and EOL;
- predicted variations in the environmental conditions;
- uncertainties in the measurement of physical parameters used in the design;
- approximations or uncertainties in the models of the sensors, actuators, plant or the environment used in the design;
- approximations in the implementation of the controller such as numerical round-off errors.

5.4.5.4
The controller design shall be compatible with operational requirements such as

a. autonomy with respect to the ground;

b. observability from the ground;

c. delay in ground reaction due to transmission delays or availability of ground equipment or operators;

d. capability for in-flight reprogramming by uploading the S/W patches.

5.4.5.5
The controller design shall be compatible with a given set of potential failures (defined in agreement with the system engineering) in order to

a. enable detection and identification of those failures either autonomously or from the ground;

b. enable a recovery after occurrence of those failures (no loss of mission);

c. meet the performance specified after the occurrence of those failures.

5.5 Verification and validation

5.5.1 General

The control engineering verification and validation process is a part of the system verification and validation process and therefore is consistent with the verification requirements defined in ECSS-E-10 Part 1 and ECSS-E-10 Part 2.

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.

5.5.2 Definition of control verification strategy

5.5.2.1
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).

5.5.2.2

The strategy for the verification of the control objectives shall be defined in consistency with the system verification plan.

5.5.2.3

The strategy for the verification of the control objectives shall be able to demonstrate that all the controlled system requirements are met.

5.5.2.4

A plan for the verification and validation of the controlled system shall be developed and documented, as specified in 5.5.2.6 and Annex E.

NOTE This can be part of the system verification plan.

5.5.2.5

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

5.5.2.6

The controlled system verification plan shall conform to and include:

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

b. the methods used to verify the requirements (e.g. reduced or full performance simulation, equipment level testing, and open-loop and closed-loop testing with or without H/W-in-the-loop);

c. a description of the control engineering verification and validation tasks;

d. the resources, responsibilities and schedule;

e. a description of the procedures, tools and facilities for verification;

f. the model philosophy.

5.5.2.7

The CE verification tasks shall be phased to be consistent with the tasks for the verification of the lower levels (control system components) and upper levels (controlled system level).

5.5.2.8

The strategy for validation of the models and tools used for the controlled system verification shall be included in the CE verification plan.

5.5.3 Preliminary verification of performance

5.5.3.1

To reduce risks, the control verification process shall start early in the project to validate the control concepts and design as they become available.

5.5.3.2

The verification of critical features shall be performed during the design and development phases, relying on simulation models or development models (prototypes).

5.5.3.3
The representativity and accuracy of the simulation models and tools used for the verification shall be assessed.

NOTE The process can be iterative according to the design maturity.

5.5.4 Final functional and performance verification

5.5.4.1 Verification by analysis

a. The performance of the controlled system shall be demonstrated by closed-loop analysis based on the use of system representative simulation models.

b. The controlled system performance shall be demonstrated in defined worst cases w.r.t system dynamical and geometrical conditions, including FDIR resulting conditions.

c. The verification shall cover all operational configurations of control modes and sensors-actuators, including back-up configurations.

d. Verification by analysis shall be supported by H/W testing.

EXAMPLE Correlation of the sensor mathematical model parameters with H/W tests.

5.5.4.2 Verification with flight H/W and S/W

a. The function and performance of the flight hardware components of the control system shall be verified.

b. Numerical accuracy of the control S/W on the target H/W (or emulator) shall be verified.

EXAMPLE The numerical accuracy can be verified by hardware-in-the-loop tests or comparison with numerical simulations.

c. The control verification process should include functional validation in closed-loop tests with flight S/W and flight H/W models or flight representative models.

d. The real sensors should be stimulated by the EGSE.

NOTE The stimuli can be electrical (test connector) or physical (detector level).

e. Mode transitions including FDIR mechanisms shall be tested and verified according to the verification plan.

f. After final integration, polarity of the sensors and actuators shall be verified.

5.5.5 In-flight validation

When in-flight validation is specified, ground observability of the controlled system shall be capable of enabling validation.

(This page is intentionally left blank)

Annex A (normative)

Control engineering documentation

A.1 General

A.1.1

The objective of this Annex is to define the specific documents for control engineering as addressed in Clause 5.

A.1.2

a. For information and documentation management, the requirements in ECSS-M-50, tailored as per project-specific DRL and DRD, shall be applied.

b. All documents issued in the framework of CE activities, during all the project phases, shall be consistent with Table 2 to Table 5.

A.2 Document requirements list

Table A-1 defines the general requirements w.r.t. the control engineering documentation as follows:

a. Documents marked with R (responsible) shall be produced.

b. Documents marked with C (contributing) shall be supported.

NOTE The document list is structured according to the following classification:

E – Control system engineering;

V – Assembly, integration and verification;

G – Ground support equipment;

O – Flight operations.

Table A-1: Control engineering document requirements list

No.	Title	R-C	Remark
E	**Control system engineering**		
E-1	Controlled system specification	C	This can be part of system specification
E-2	Control system design report	R	Including control related part of equipment
E-3	Controlled system analysis report	R	
E-4	Specification of compliance and requirement assessment report	C	This can be part of E-2
E-5	Control related development plan	C	Input to system engineering plan
E-6	System performance synthesis	C	
E-7	System budgets	C	
E-8	Interface control documents (H/W and S/W)	C	
E-9	Control algorithms specification	R	Input to controller H/W or S/W implementation
E-10	Control related equipment specifications	C	
E-11	CE PA-related documentation (e.g. FMECA, worst case analysis)	C	According to ECSS-Q-20
V	**Assembly, integration and verification**		
V-1	Controlled system verification plan	R	This can be part of system SEP/AIV plan
V-2	Controlled system test specifications and procedures	C	This can be part of system test specifications and procedures
V-3	Controlled system test reports	C	This can be part of system test reports
V-4	Controlled system verification report	R	This can be part of system verification report
G	**Ground support equipment**		
G-1	Control related MGSE requirements specification	C	Including MGSE test requirements
G-2	Controlled system EGSE requirements specification	C	Including EGSE test requirements
G-3	Controlled system EGSE design report (w.r.t. e.g. simulation models, stimuli)	C	Including H/W and S/W architectural and detailed design
G-4	Controlled system EGSE test procedures	C	
G-5	Controlled system EGSE test reports	C	
G-6	Controlled system GSE user manual	C	Including operation and maintenance

Table A-1: Control engineering document requirements list *(continued)*

No.	Title	R-C	Remark
O	**Flight Operations**		
O-1	Inputs to system operation documentation (e.g. launcher requirements, timeline, operational constraints, malfunction procedures)	C	See ECSS-E-70 Part 1 and ECSS-E-70 Part 2
O-3	Controlled system data base	C	This can be part of System data base
O-4	Controlled system users manual (including Operating procedure, contingency analysis and procedures)	C	This can be part of System users manual
O-5	Controlled system in-flight performance evaluation report	C	This can be part of System performance evaluation report

A.3 Document requirements definition

The following apply to the DRDs covered in Annex B to F, that define the set of information to be provided in the course of a control system design, development, verification and validation:

a. The depth of the contents and analyses should be tailored according to the development status of the system.

b. For practical reasons, the contents need not be found in a single document but may be allocated to a set of separate documents or documents may be combined (especially for early project phases).

(This page is intentionally left blank)

Annex B (normative)

Control system design report (CSDR) DRD

B.1 DRD identification

B.1.1 Requirement identification and source document

ECSS-E-60A, Annex A.2 (see also Tables 3, 4 and 5)

B.1.2 Purpose and objective

The control system design report (CSDR) provides:

- The detailed description of the control system design (consisting of sensors, actuators and the controller). It includes also information on the plant to be controlled (e.g. basic description of plant, parameters, assumptions and constraints and disturbances) which are relevant for the control design.
- Budget type information which summarises control related aspects (e.g. pointing error budget).
- Control design justification and compliance statements to the control relevant requirements.

A CSDR is issued at major milestones in the development of a space control system (e.g. design review).

The CSDR is prepared on the basis of the applicable specifications and requirement documents.

The CSDR is part of the overall system design description and is, therefore, closely related to the overall system engineering documentation. Thus the CSDR has many interrelations to other engineering disciplines such as mechanical design, electrical design, operations and software design and their related documentation.

B.2 Expected response

B.2.1 Response identification

The requirements for project identification contained in ECSS-M-50 shall be applied to the CSDR.

B.2.2 Scope and content

The CSDR shall provide the information presented in the following sections:

<1> Introduction

The CSDR shall contain a description of the purpose, objective, content and the reason prompting its preparation.

<2> Applicable and reference documents

The CSRD shall list the applicable and reference documents to support the generation of the document.

<3> Terms and definitions, abbreviated terms and symbols

The CSRD shall include any additional definitions, abbreviations or symbols used.

<4> Summary and understanding of controlled system requirements

(a) The CSRD shall summarize the key requirements for the controlled system.

(b) The CSRD should summarize the discussion on the understanding and clarification of requirements.

(c) If the control performance requirements are part of system requirements (e.g. pointing performance of an antenna), the CSRD should explicitly state them.

<5> Controlled system overview

(a) Plant configuration.

The CSRD shall provide an overview of the plant to be controlled including, as a minimum, the following:

(1) plant description;

(2) physical parameters;

(3) reference frames and sign conventions;

(4) external disturbances.

(b) Control system architecture.

This subclause shall describe the overall control system architecture including, as a minimum, the following:

(1) functional architecture;

- nominal functions;
- failure management (redundancy concept and FDIR approach);

(2) operational architecture (control modes and mode transitions);

(3) implementation architecture (sensors, actuators and controller);

(4) system interfaces (on-board system interface and ground segment interface).

<6> Sensors and actuators description

(a) Technical baseline.

The CSRD shall describe the technical baseline of the sensors and actuators, including, as a minimum, the following:

(1) description of measurement and actuation principle;

(2) description of sensor-actuator modes;

(3) physical parameters;

(4) sensor and actuator interfaces (e.g. resolution, timing and noise).

(b) Sensors and actuators accommodation and constraints

The CSRD shall state and describe the constraints for accommodation of the sensors and actuators (e.g. blinding of optical sensors, stiffness between sensor and actuator mounting).

<7> Controller description

(a) Control mode overview.

The CSRD shall:

(1) Provide an overview on the control modes, identifying and describing all control modes and the transitions between the control modes.

(2) Describe the conditions for the transitions.

(3) Document the control mode in form of diagrams or tables and explanatory text.

(b) Control mode description.

The CSRD shall describe each control mode (nominal and failure cases) including, as a minimum, the following:

(1) mode functional and performance requirements;

(2) plant, sensors and actuators configuration;

(3) control functions (e.g. overview and diagrams);

(4) control algorithms (brief description).

NOTE As specified in Annex C the detailed definition of the control algorithms is included in the "Control algorithms specification".

(c) System interface.

The CSRD shall describe the interface to the higher level system in terms of commands to the controller and feedback information from the controller.

NOTE Usually, for a S/W based control implementation, the system interface is defined as telemetry and telecommand interface (TM/TC). In this case, only an overview of the TM/TC is given; and as specified in Annex C, the detailed definition of the TM/TC interface is included in the "Control algorithms specification".

<8> Operational constraints of control system

(a) Basic control system operations.

The CRDS shall:

(1) Describe the basic control system operations from start-up and initialization to shutdown of the control system.

(2) List all operational constraints for the control system.

(b) Description of in-flight calibration procedures.

The CSRD shall list and describe in-flight calibration procedures.

(c) Required ground S/W support functions and algorithms

The CSRD shall list and describe ground S/W support functions and algorithms for the operation of the control system (e.g. pre-processing of parameters for upload, supporting functions for calibration parameter calculations).

<9> Control system design justification summary

(a) Main trade-offs.

The CSRD shall describe the main control system trade-offs.

(b) Baseline concept selection.

The CSRD shall describe the motivation for the control system baseline selection.

(c) Heritage.

The CSRD shall describe the heritage of a selected control system concept including the experience gained from former projects.

<10> Control budgets summary

The CSRD shall document all budgets which are performed during the control development process.

NOTE Usually all control systems deal with different error sources which influence the specified performance. These error sources are usually handled as error budgets (e.g. pointing error budget).

<11> Compliance to control requirements

The CSRD shall document the compliance to the control system requirements.

NOTE The synthesis of the control system verification is documented in the “Controlled system verification report”, (see DRD in Annex F).

Annex C (normative)

Control algorithms specification (CAS) DRD

C.1 DRD identification

C.1.1 Requirement identification and source document

ECSS-E-60A, Annex A.2 (see also Tables 3 and 4).

C.1.2 Purpose and objective

A control algorithms specification (CAS) provides the detailed information about the control algorithms to be implemented in the controller of a space control system.

Usually this information is an input to the corresponding on-board software specification (in cases where the control algorithms are implemented in software), however, since the controller can also be implemented in hardware the control algorithms specification are applicable to this option too. Consequently the control algorithms specifications do not contain software specific requirements (e.g. memory size, type of variable access).

The CAS is issued as input to the relevant on-board software or hardware specifications. An initial version serves as the baseline for the procurement of controller H/W and S/W. Later updated versions are issued to track any change in the control algorithms design. The final version is issued at the end of the development and verification process in line with the latest version of the on-board software or hardware.

The CAS is prepared on the basis of the applicable specifications and requirement documents.

The CAS is usually closely related to the corresponding on-board software specification and may be treated as an annex to the on-board software specification.

C.2 Expected response

C.2.1 Response identification

The requirements for project identification contained in ECSS-M-50 shall be applied to the CAS.

C.2.2 Scope and content

The CAS shall provide the information presented in the following sections:

<1> **Introduction**

The CAS shall contain a description of the purpose, objective, content and the reason prompting its preparation.

<2> **Applicable and reference documents**

The CAS shall list the applicable and reference documents to support the generation of the document.

<3> **Terms and definitions, abbreviated terms and symbols**

The CAS shall include any additional definitions, abbreviations or symbols used.

<4> **Controller functional architecture**

(a) The CAS shall describe the controller functional architecture, i.e. a decomposition of the controller into functions and sub-functions.

(b) The controller functional architecture shall include, as a minimum, the following:

(1) overview of functional architecture;

(2) definition of functions;

(3) description of interfaces between functions (inputs, outputs);

(4) description of controller external interfaces;

(5) timing requirements of functions (e.g. frequency, delays and order of execution).

(c) The overview controller functional architecture shall be documented with diagrams showing the date and control flow between the single control functions.

<5> **Specification of single control functions**

(a) The CAS shall describe each control function individually.

NOTE Examples of functions are:

- sensor data processing (e.g. filtering, sensor fusion);
- control laws;
- actuator commands processing (e.g. thruster selection);
- control related FDIR;
- mode management;
- control related TM/TC management;
- control related housekeeping;
- support functions (e.g. mathematics and transformations).

(b) Each control function shall be described by the following items:

(1) algorithms (including the specified numerical precision);

(2) inputs-outputs;

(3) parameters (including default settings);

(4) internal states (including initial conditions).

(c) The algorithms shall be described by mathematical formulas.

NOTE Block oriented documentation of tools or pure code can be added to the mathematical formulas.

<6> List of parameters and states

(a) List of commandable parameters and states.

The CAS shall describe the parameters and states which can be set by external commands (for ground testing and in flight operation).

(b) List of observable parameters and states.

The CAS shall describe the parameters and states to be observed (for ground testing and in flight operation).

(c) List of default flight parameters and initial conditions.

The CAS shall describe the default flight parameters and initial conditions.

(This page is intentionally left blank)

Annex D (normative)

Controlled system analysis report (CSAR) DRD

D.1 DRD identification

D.1.1 Requirement identification and source document

ECSS-E-60A, Annex A.2 (see also Tables 3, 4 and 5).

D.1.2 Purpose and objective

A controlled system analysis report (CSAR) provides the details on the analysis done for a space control system.

The objectives of the controlled system analysis report are:

- to document the controller design process (as specified in Annex C, the detailed control algorithms design are documented on the control algorithms specification);
- to demonstrate that the controlled system meets all its performance requirements.

Usually, an analysis of the control system is of one of the following types:

- analytical-numerical calculations;
- numerical simulations;
- control related budgets.

All these types of analyses are documented in the CSAR.

The CSAR is issued in several phases of the project, usually at the end of each project phase. The final version of the CSAR takes into account the final design of the control system and the plant.

The CSAR is prepared on the basis of the applicable specifications and requirement documents. The CSAR is an input to the controlled system verification plan (see Annex F) and documents all analyses which demonstrate that the control performance is met.

D.2 Expected response

D.2.1 Response identification

The requirements for project identification contained in ECSS-M-50 shall be applied to the CSAR.

D.2.2 Scope and content

The CSAR shall provide the information presented in the following sections:

<1> **Introduction**

The CSAR shall contain a description of the purpose, objective, content and the reason prompting its preparation.

<2> **Applicable and reference documents**

The CSAR shall list the applicable and reference documents to support the generation of the document.

<3> **Terms and definitions, abbreviated terms and symbols**

The CSAR shall include any additional definitions, abbreviations or symbols used.

<4> **Analytical-numerical calculations**

(a) The CSAR shall describe, individually, each separate analysis based on analytical-numerical calculations.

(b) The analytical-numerical calculation based analysis shall be described by the following items:

(1) description of used method;

(2) description of calculation tool;

(3) description of formulas and numerical parameters;

(4) analysis results (e.g. controller structure and parameters, performance, stability, robustness and mode transitions behaviour).

<5> **Numerical simulations**

(a) Description of simulation tools

The CSAR shall describe the used simulation tools.

(b) Description of simulation models

The CSAR shall describe the used simulation models including, as a minimum, the following:

(1) standards used;

(2) description of mathematical model (functions, algorithms and numerical parameters):

- plant configuration (numerical values, range of parameters and uncertainties);
- environment (in particular external disturbances);
- sensors and actuators;

(3) documentation of simulation model (model implementation);

(4) numerical integration method.

(c) Control simulations results

The CSAR shall describe separately the evaluation of each simulation result (e.g. for each mode including nominal and failure cases).

NOTE Examples of types of simulations are:

- control performance simulations;
- robustness and sensitivity simulations (stability margins, sensitivity against parameter variations and range of applicability);
- mode transitions simulations.

<6> Control related budgets

(a) The CSAR shall document separately each control related budget.

(b) The control related budget shall be described including, as a minimum, the following:

(1) budget methodology (e.g. root mean square, bias and power spectrum);

(2) analysis of individual contributors (indicating source of data);

(3) overall budget.

(c) The overall budget referred to in (b)(3) above should be in form of a table.

(This page is intentionally left blank)

Annex E (normative)

Controlled system verification plan (CSVP) DRD

E.1 DRD identification

E.1.1 Requirement identification and source document

ECSS-E-60A, Subclause 5.5.2.4 and Annex A.2.

E.1.2 Purpose and objective

The controlled system verification plan (CSVP) provides an overview of the control verification and validation strategy (including a description of constraints and boundary conditions) and the detailed planning information on all the verification steps of the controlled system requirements.

Usually the verification of control related requirements can be done by analysis or by test. The CSVP documents specifically the strategy and logic used to determine the requirements that are verified by analysis, those that are verified by test and those that are verified with a combination of both.

The CSVP is issued in several phases of the project starting in Phase B and updated and at major project review milestones.

Since the control related requirements are often identical to system requirements, the CSVP is in line with the overall system verification planning defined in the system verification plan (DRD of ECSS-E-10 Part 1).

E.2 Expected response

E.2.1 Response identification

The requirements for project identification contained in ECSS-M-50 shall be applied to the CSVP.

E.2.2 Scope and content

The CSVP shall provide the information presented in the following sections:

<1> Introduction

The CSVP shall contain a description of the purpose, objective, content and the reason prompting its preparation.

<2> Applicable and reference documents

The CSVP shall list the applicable and reference documents to support the generation of the document.

<3> Terms and definitions, abbreviated terms and symbols

The CSVP shall include any additional definitions, abbreviations or symbols used.

<4> Definition of control verification and validation strategy

(a) Verification and validation logic.

The CSVP shall describe:

(1) the logic of the control related verification process;

(2) the underlying model philosophy (e.g. tests on test bed, EM or FM level).

(b) Verification and validation constraints.

The CSVP shall describe the constraints under which the verification and validation logic is set up.

NOTE Major constraints can be due to the availability and feasibility of test facilities, the incompatibility of the controlled system with the test environmental conditions (e.g. 1-g compatibility, thermal vacuum).

(c) Verification and validation by analysis.

The CSVP shall give an overview of the planned analyses.

(d) Verification and validation by test.

(1) The CSVP shall give an overview of the planned tests.

(2) The tests level shall be indicated for each test (e.g. S/W level, equipment level, control system level and system level).

<5> Definition of control verification plan

(a) Definition of planned analyses.

The CSVP shall describe the planned analyses including, as a minimum, the following:

(1) objectives and conditions;

(2) analysis methods;

(3) used models;

(4) used tools.

(b) Definition of planned tests

The CSVP shall describe the planned tests including, as a minimum, the following:

(1) objectives and conditions;

(2) test type characterization, e.g.

- S/W-in-the-loop, H/W-in-the-loop;
- open-loop, closed-loop;
- sign checks;
- timing tests.

(c) Description of test environments.

The CSVP shall describe for each test the planned test environment including, as a minimum, the following:

(1) test set-up;

(2) scope, range and accuracy of test equipment;

(3) validation of test equipment;

(4) evolution of the test environment (e.g. replacement of simulated functions by real units).

(This page is intentionally left blank)

Annex F (normative)

Controlled system verification report (CSVR) DRD

F.1 DRD identification

F.1.1 Requirement identification and source document

ECSS-E-60A, Annex A.2 (see also Tables 3 and 4).

F.1.2 Purpose and objective

The controlled system verification report (CSVR) provides the summary information assuring that all controlled system requirements are verified (either by analysis or by test or by a combination of both).

The single analysis or test results can be documented by the corresponding analysis and test reports. The CSVR summarizes these single analysis and results and provides a correlation between analysis and test.

The CSVR documents the synthesis of the achieved controlled system performance and all control related nonconformances, not closed during the development.

The CSVR is issued in several phases of the project starting in Phase B and updated and at major project review milestones. In an early project phase (starting from Phase B), the CSVP can only rely on analysis results to predict the control performance while at the end of the development (Phase D) the CSVP includes all relevant test results.

Since the control related requirements are often identical to system requirements the CSVR is in line overall system verification documentation defined in the system verification report (DRD of ECSS-E-10 Part 1).

F.2 Expected response

F.2.1 Response identification

The requirements for project identification contained in ECSS-M-50 shall be applied to the CSVR.

F.2.2 Scope and content

The CSVR shall provide the information presented in the following sections:

<1> Introduction

The CSVR shall contain a description of the purpose, objective, content and the reason prompting its preparation.

<2> Applicable and reference documents

The CSVR shall list the applicable and reference documents to support the generation of the document.

<3> Terms and definitions, abbreviated terms and symbols

The CSVR shall include any additional definitions, abbreviations or symbols used.

<4> Verification results

(a) Summary of analysis results.

The CSVR summarizes in a systematic way all controlled system analyses defined in the CSVP.

(b) Summary of test results.

The CSVR shall summarize in a systematic way all controlled system tests defined in the CSVP.

(c) Correlation of analysis and test results.

(1) The CSVR shall document the comparison between analysis and test results, taking into account the different constraints and conditions of the analyses and the tests.

(2) The evaluation of the deviations between analysis and test results shall be described and documented.

(d) Summary and synthesis of results

The CSVR shall provide a summary and a synthesis of the overall verification results.

<5> Close-out of controlled system requirements

(a) Inputs to system verification matrix

(1) The CSVR shall describe the inputs for the system verification matrix.

(2) The association of each system level control requirement with the relevant analyses and tests which prove that the requirement is met shall be documented.

(b) Control related nonconformances

(1) The CSVR shall document all control related nonconformances, not closed at the end of the actual development phase.

(2) The nonconformances specified in (1) above shall include nonconformances to system level requirements (e.g. controlled system performance requirements) and any other nonconformances which affect the system behaviour in an unacceptable way.

Bibliography

ECSS-E-00	Space engineering — Policy and principles
ECSS-E-10 Part 2 [1]	Space engineering — Verification
ECSS-E-10-04	Space engineering — Space environment
ECSS-E-20	Space engineering — Electrical and electronic
ECSS-E-30 Part 1	Space engineering — Mechanical — Part 1: Thermal control
ECSS-E-30 Part 2	Space engineering — Mechanical — Part 2: Structural
ECSS-E-30 Part 3	Space engineering — Mechanical — Part 3: Mechanisms
ECSS-E-30 Part 4 [1]	Space engineering — Mechanical — Part 4: ECLS
ECSS-E-30 Part 5 [1]	Space engineering — Mechanical — Part 5: Propulsion
ECSS-E-30 Part 6	Space engineering — Mechanical — Part 6: Pyrotechnics
ECSS-E-30 Part 7	Space engineering — Mechanical — Part 7: Mechanical parts
ECSS-E-30 Part 8	Space engineering — Mechanical — Part 8: Materials
ECSS-E-40 Part 1	Space engineering — Software — Part 1: Principles and requirements
ECSS-E-50 Part 1	Space engineering — Communications — Part 1: Principles and requirements
ECSS-E-70 Part 1	Space engineering — Ground systems and operations — Part 1: Principles and requirements
ECSS-M-00-02	Space project management — Tailoring of space standards
ECSS-M-30	Space project management — Project phasing and planning
ECSS-M-40	Space project management — Configuration management
ECSS-Q-20	Space product assurance — Quality assurance
ESA-NCR-502,	ESA Pointing Error Handbook, Issue 1, February 1993

1) To be published.

(This page is intentionally left blank)

ECSS Document Improvement Proposal

1. Document I.D. ECSS-E-60A	**2. Document date** 14 September 2004	**3. Document title** Control engineering
4. Recommended improvement (identify clauses, subclauses and include modified text or graphic, attach pages as necessary)		
5. Reason for recommendation		
6. Originator of recommendation		
Name:	Organization:	
Address:	Phone: Fax: e-mail:	**7. Date of submission:**
8. Send to ECSS Secretariat		
Name: W. Kriedte ESA-TEC/QR	Address: ESTEC, P.O. Box 299 2200 AG Noordwijk The Netherlands	Phone: +31-71-565-3952 Fax: +31-71-565-6839 e-mail: Werner.Kriedte@esa.int

Note: The originator of the submission should complete items 4, 5, 6 and 7.

An electronic version of this form is available in the ECSS website at: http://www.ecss.nl/
At the website, select “Standards” - “ECSS forms” - “ECSS Document Improvement Proposal”

(This page is intentionally left blank)