**ECSS-E-HB-60A**
14 December 2010

# Space engineering

## Control engineering handbook

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

## Foreword

This Handbook is one document of the series of ECSS Documents intended to be used as supporting material for ECSS Standards 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.

Best practises in this Handbook are defined in terms of what can 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 and Handbooks.

This Handbook was reviewed by the ECSS Executive Secretariat and approved by the ECSS Technical Authority.

## Disclaimer

ECSS does not provide any warranty whatsoever, whether expressed, implied, or statutory, including, but not limited to, any warranty of merchantability or fitness for a particular purpose or any warranty that the contents of the item are error-free. In no respect shall ECSS incur any liability for any damages, including, but not limited to, direct, indirect, special, or consequential damages arising out of, resulting from, or in any way connected to the use of this document, whether or not based upon warranty, business agreement, tort, or otherwise; whether or not injury was sustained by persons or property or otherwise; and whether or not loss was sustained from, or arose out of, the results of, the item, or any services that may be provided by ECSS

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

# Change log

| | |
|---|---|
| ECSS-E-HB-60A<br>14 December 2010 | First issue<br>This Handbook is based on ECSS-E-60A Standard (2004). The technical content was kept and where necessary the formulation was adapted to comply with the drafting rules for ECSS Handbooks. |

# Table of contents

## Figures

## Tables

# 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 and handbooks. This Handbook is not intended to duplicate them.

This Handbook focuses on the specific issues involved in control engineering and is intended to be used as a structured set of systematic engineering provisions, referring to the specific standards and handbooks of the discipline where appropriate. For this, and reasons such as the very rapid progress of control component technologies and associated “de facto” standards, this Handbook does not go to the level of describing equipment or interfaces.

This Handbook 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 Handbook are assumed to possess general knowledge of control systems engineering and its applications to space missions.

# 1
# Scope

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

It describes 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.

# 2 References

| | |
|---|---|
| ECSS-S-ST-00-01 | ECSS System – Glossary of terms |
| ECSS-E-ST-10 | Space engineering – System engineering general requirements |
| ECSS-E-ST-10-04 | Space engineering – Space environment |
| ECSS-E-ST-70 | Space engineering – Ground systems and operations |
| ECSS-Q-ST-20 | Space product assurance – Quality assurance |

# 3
# Terms, definitions and abbreviated terms

## 3.1 Terms from other documents

For the purpose of this document, the terms and definitions from ECSS-S-ST-00-01 apply.

## 3.2 Terms specific to the present handbook

### 3.2.1 actuator

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

### 3.2.2 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.

### 3.2.3 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.

### 3.2.4 control command

output of the **controller** to the **actuators** and the **sensors**

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

### 3.2.5 control component

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

### 3.2.6 control feedback

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

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

### 3.2.7 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.

### 3.2.8 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

### 3.2.9 control mode transition

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

### 3.2.10 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.

### 3.2.11 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.

### 3.2.12 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**.

### 3.2.13 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.

### 3.2.14 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**.

### 3.2.15 controlled system

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

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

### 3.2.16 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.

### 3.2.17 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 0).

### 3.2.18 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**).

### 3.2.19 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.

### 3.2.20 estimated state

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

### 3.2.21 estimator

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

### 3.2.22 guidance

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

NOTE The term is used as in GNC.

### 3.2.23 implementation

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

### 3.2.24 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.

### 3.2.25 measured state

set of variables or parameters derived from physical measurements

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

### 3.2.26 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.

### 3.2.27 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.

### 3.2.28 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.

### 3.2.29 reference state

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

### 3.2.30 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).

### 3.2.31 sensor

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

### 3.2.32 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.

### 3.2.33 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.

### 3.2.34 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 0).

### 3.2.35 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**.

## 3.3 Abbreviated terms

For the purpose of this document, the abbreviated terms from ECSS-S-ST-00-01 and the following apply:

| **Abbreviation** | **Meaning** |
|---|---|
| **3D** | three-dimensional |
| **A/D** | analogue-digital |
| **AOCS** | attitude and orbit control system |
| **A&R** | automation and robotics |
| **BOL** | beginning-of-life |

| Abbreviation | Meaning |
|---|---|
| **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 4-1 shows a general control structure. This fundamental diagram introduces the following basic concepts and definitions explained below.

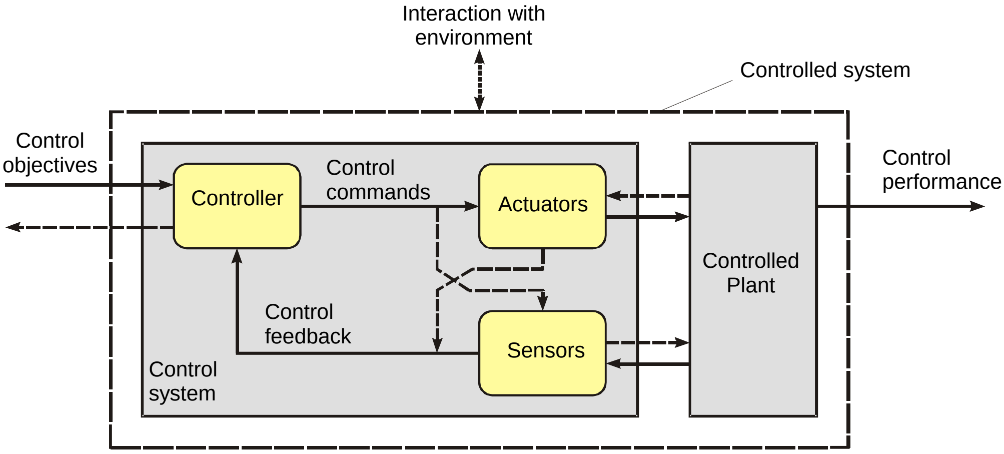

**Figure 4-1: General control structure**

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 4-1 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 handbook refers to ECSS-E-ST-70.

In the sense of classical control theory, the controller has an internal functional structure with the following functions (as shown in Figure 4-2):

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

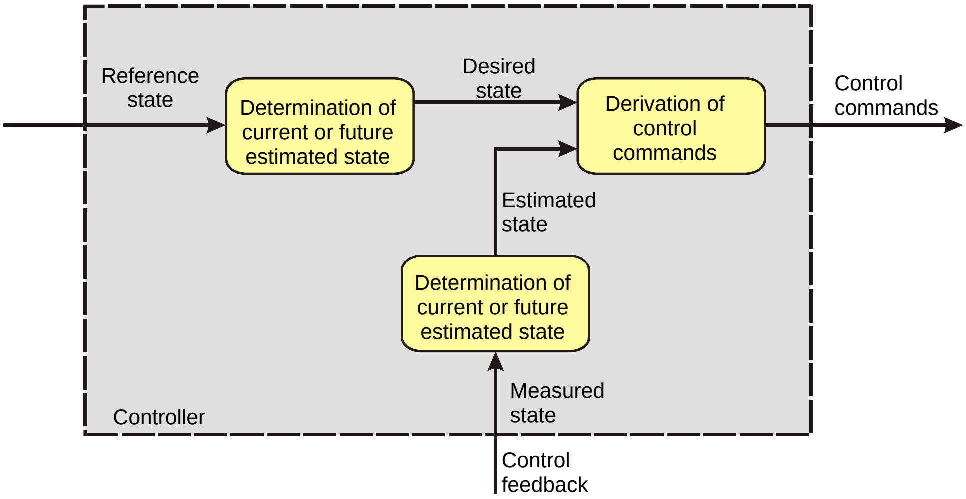
Reference state
Determination of current or future estimated state
Desired state
Derivation of control commands
Control commands
Estimated state
Determination of current or future estimated state
Measured state
Controller
Control feedback

**Figure 4-2: 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 4-2 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 4-2.

### 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-ST-10.

### 4.1.3 Organization of this Handbook

This Handbook 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, and provides a checklist of recommendations for tasks to be performed and associated expected outputs.

## 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-ST-10. 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 4-3.

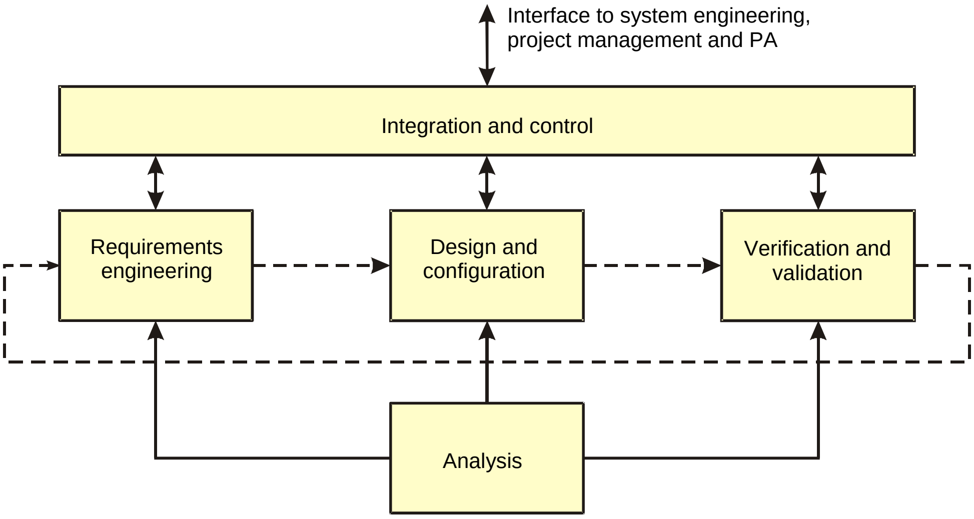
Interface to system engineering, project management and PA
Integration and control
Requirements engineering
Design and configuration
Verification and validation
Analysis

**Figure 4-3: Interaction between CE activities**

Table 4-1 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 clause 4.3;
- particularly iterative between requirements engineering, design-configuration, verification-validation and analysis.

## 4.3 Control engineering tasks per project phase

This section provides details of the engineering tasks to be performed at each phase of the project. Table 4-2 to Table 4-5 show the inputs, the tasks and the outputs for each activity.

## Table 4-1: Summary of control engineering tasks

| Control engineering activity | Specific control engineering tasks |
|---|---|
| Integration and control | - Organization and planning of control engineering activities.<br>- Contribution to system engineering database.<br>- Management of interfaces with other disciplines (e.g. mechanical engineering and software engineering) and activities (e.g. procurement and quality assurance).<br>- Contribution to human factors engineering when humans are part of the controller.<br>- Definition of budget and margin philosophy for control.<br>- Assessment of control technology and cost effectiveness.<br>- Risk management.<br>- Engineering support to control components procurement.<br>- Support to change management involving control (including in-flight maintenance).<br>- Control engineering capability assessment and resource management. |
| Requirements engineering | - Generation of control requirements from system and mission requirements.<br>- Contribution to system requirements to meet control requirements.<br>- Allocation of control requirements to sub-assemblies or equipment (sensors, actuators and controller H/W).<br>- Definition of control S/W requirements.<br>- Definition of control interface requirements between control components.<br>- Definition of control operations requirements.<br>- Definition of control verification requirements. |
| Analysis | - Selection of adequate analysis tools and methodologies.<br>- Requirements evaluation and budgets breakdown.<br>- Disturbances evaluation.<br>- 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.<br>- Numerical analysis to support the control design.<br>- Performance verification analysis (including simulation).<br>- Numerical analysis to support in-flight evaluation. |
| Design and configuration | - Definition of functional control architecture (including functional interfaces).<br>- Definition of operational control architecture (modes).<br>- Definition of physical control architecture (H/W, S/W and human operation).<br>- Design of control concepts and algorithms.<br>- Control design trade-offs.<br>- Generation of control budgets.<br>- Contribution to selection and procurement of control components.<br>- Contribution to system configuration management. |
| Verification and validation | - Definition of control verification and validation strategy (including specification of requirements for test environments).<br>- Definition of control verification and validation strategy.<br>- Preliminary verification of performance by analysis or prototyping.<br>- Final functional and performance verification by analysis.<br>- Final verification and validation of controlled system (H/W, S/W and human operation) by hardware-in-the-loop tests.<br>- In-flight validation of controlled system behaviour. |

Table 4-2: 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<br>- System development approach and constraints | - System objectives<br>- Mission requirements<br>- System performance requirements | - Controlled system objectives<br>- 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<br>- Generation of inputs to the system development approach<br>- Identification of availability and maturity of control technology | - Translate mission and system objectives into preliminary control objectives<br>- Definition of preliminary control requirements<br>- Control system life cycle definition | - Analysis of control requirements feasibility for control system alternatives<br>- Preliminary disturbances evaluation<br>- Preliminary performance assessment<br>- Initial sensitivity analysis<br>- Identification of control system critical aspects | - Establishment and trade-off of control system design concepts<br>- Establishment of control system design baseline (including preliminary FDIR concept) | - Control engineering support for definition of verification and validation concepts<br>- Preliminary definition of control verification and validation methods and strategies |
| **Outputs** | - Inputs to project and system engineering plan<br>- Inputs to cost estimates and schedule estimates<br>- 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 4-3: 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<br>- Control life cycle Phase 0/A | - System objectives<br>- Mission requirements<br>- Controlled system objectives and requirements | - Phase 0/A simulation models<br>- Phase 0/A control analyses | - Phase 0/A control design | - System verification plan<br>- Phase 0/A control verification plan |
| **Tasks** | - Update control system inputs to system engineering management plan and cost estimates (including risk management)<br>- Review of the control systems compatibility with the system design and constraints | - Analyse system requirements<br>- Generate controlled system requirements<br>- Allocate controlled system requirements to subsystems and components<br>- Check traceability of control requirements with respect to system requirements | - Analysis of control requirements for sub-systems and components<br>- Disturbances assessment<br>- Controlled system performance analysis<br>- Controlled system sensitivity analysis<br>- Assessment of control technologies for early prototyping | - Definition of control system baseline<br>- Allocation of control system functions to H/W, S/W and human operators (in-flight and on ground)<br>- Definition of control system interfaces<br>- Preliminary design of controller (control laws)<br>- Preliminary definition of control related FDIR<br>- Selection of control components and technologies<br>- Establishment of control related budgets and margins | - Prepare controlled system verification plan<br>- Provide inputs to lower level verification plans<br>- Provide inputs to the management plan<br>- Support Phase C/D verification planning |
| **Outputs** | - Inputs to project and system engineering plan<br>- Inputs to cost estimates and schedule | - Inputs to system or subsystem technical specifications<br>- Inputs to lower level technical specifications<br>- Inputs to requirements database<br>- Inputs to interface control documents | - Controlled system analysis report (including simulation models description) | - Control system design report (incl. design justification)<br>- Preliminary control algorithms specification<br>- Preliminary control system budgets | - Controlled system verification plan<br>- Preliminary controlled system verification report |

Table 4-4: 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<br>- Control life cycle Phase B | - Phase B control objectives and requirements<br>- Phase B control components specifications | - Phase B simulation models<br>- 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)<br>- Management of required control system changes<br>- Support of operations<br>- Review of data packages<br>- Support to Phase E/F planning and cost estimate | - Update of specifications<br>- Review and assessment of control requirements changes<br>- Review and assessment of system changes related to control | - Detailed controlled system performance analysis<br>- Update of sensitivity analysis<br>- Support to verification process<br>- Support to in-flight verification process definition | - Update of the control design baseline<br>- Finalization of control system functional architecture and interfaces<br>- Detailed design of controllers and optimization of controller parameters<br>- Detailed design of control-related FDIR<br>- Review of control budget and margins analysis | - Co-ordinate and monitor controlled system and lower level verification plans and activities<br>- Monitor lower level verification acceptance activities<br>- Support and monitor lower level qualification and acceptance tests<br>- Perform controlled system qualification and acceptance tests |
| **Outputs** | - Updated inputs to project and system engineering plan<br>- Inputs to system database<br>- Inputs to operations handbook or user manual<br>- Updated inputs to cost estimates for Phase E/F | - Updated inputs to system or subsystem technical specifications<br>- Updated inputs to lower level technical specifications<br>- Updated inputs to interface control documents | - Controlled system analysis report<br>- Inputs to the definition of the strategies for the in-flight calibration and performance analysis | - Final control system design report<br>- Final control algorithms specification (including control system TM/TC specification)<br>- Final control system budgets | - Controlled system verification report<br>- Inputs to in-flight verification plan |

**Table 4-5: 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<br>- Controlled system in-flight performance data<br>- Strategies for the in-flight performance analysis | - Final control system design report | - In-flight verification plan |
| **Tasks** | - Support of system operations<br>- Management of specified controller changes<br>- Control engineering support to system disposal<br>- Generation of lessons learnt for control engineering | - Comparison of control objectives and requirements with controlled system performance<br>- Clarify control objectives and requirements changes during operation | - Analysis of controlled system operational performance<br>- Analysis of required controller changes | - Update of controller design (in case of required changes) | - Support controlled system operational performance verification<br>- Support system review |
| **Outputs** | - Inputs to disposal plan | - New control related operational requirements | - Inputs to controlled system operational performance report<br>- Updated control controlled system analysis report<br>- Inputs to payload data evaluation | - Controller design updates (updated control system design report) | - Inputs to in-flight acceptance report<br>- Inputs to periodic mission reports |

# 5 Control engineering process recommendations

## 5.1 Integration and control

### 5.1.1 General

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

Integration and control can be consistent with the system engineering plan (SEP) and system engineering integration and control requirements.

### 5.1.2 Organization and planning of CE activities

Control engineering contributes to the system engineering management plan to define, organize and plan all control engineering activities to achieve the specified control performance. This applies especially to the control development and verification logic which is closely related to the system design and development planning.

Control engineering contributes to and participates 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

Control engineering provides inputs to the system engineering database concerning controller data, and control related sensor and actuator parameters (e.g. flight dynamics database).

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

### 5.1.4 Management of interfaces with other disciplines

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

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

- mechanical interfaces (e.g. mass properties, alignment, stiffness, eigenfrequencies and micro-vibrations);
- thermal interfaces;
- software interfaces (control functions realized by S/W);
- ground segment interfaces;
- operational interfaces;
- TT&C;
- optical.

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

### 5.1.5 Contribution to human factors engineering

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

- human performance capabilities;
- man-machine interfaces;
- training of control operators.

### 5.1.6 Budget and margin philosophy for control

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

### 5.1.7 Assessment of control technology and cost effectiveness

The programmatic risk w.r.t. the maturity of the control related technology is analysed and assessed, in particular with respect to controller (e.g. H/W – S/W – human and analogue-digital), and sensors and actuators.

The effort (cost and risk) for the verifications of the control objectives and requirements is also assessed.

### 5.1.8 Risk management

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

### 5.1.9 Support to control components procurement

Control engineering supports system engineering for the procurement of the controller H/W and S/W, and for the procurement of sensors and actuators.

### 5.1.10 Support to change management involving control

Control engineering:

- supports the management of nonconformances related to control.
- handles changes related to controller design and implementation.
- reviews changes in control related disciplines.

### 5.1.11 Control engineering capability assessment and resource management

Control engineering assesses the control related capability and experience, and performs the related resource management w.r.t. human resources, and 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).

    NOTE 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

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

The control requirements are allocated to lower level requirements for the control components (controller, sensors and actuators). The allocation is usually an iterative process, supported by:

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

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

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

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

Through an appropriate document (e.g. ICD), control engineering defines and justifies 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

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

#### 5.2.3.1 Sensors

The following sensor properties can be defined:

- Functional and performance requirements (possibly specified separately for the different modes)
  - measurement principle (analogue-digital)
  - absolute-relative accuracy (before-after calibration)
  - measurement range (including limitations imposed by operating conditions)
  - resolution
  - linearity
  - maximum allowed unpredictable bias
  - measurement bandwidth
  - timing requirements (e.g. sampling rate, maximum delay time, and maximum time jitter for sampling rate and delay)
  - maximum allowed noise, including quantization noise from A/D conversion (RMS, PSD)
  - FDIR requirements
- Operational requirements
  - 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

- Configuration requirements
  - accommodation requirements (e.g. free field of view, and minimum stiffness between actuators and sensors)
  - disturbance constraints from internal sources (e.g. vibrations)
- Interface requirements
  - alignment requirements (bias and stability)
  - electrical interface requirement (e.g. maximum noise for analogue interfaces)
  - data interface requirement (e.g. resolution)
- Verification requirements
  - test interface requirements (stimuli inputs)
  - special provisions for ground testing

All properties of the sensors can be checked for feasibility.

#### 5.2.3.2 Actuators

The following actuator properties can be defined:

- Functional and performance requirements (possibly specified separately for the different modes)
  - actuation principle
  - absolute-relative accuracy (before-after calibration)
  - operating range (including limitations by operating conditions)
  - resolution
  - linearity
  - maximum allowed unpredictable bias
  - actuation bandwidth for various defined control command points, response time and settling time (step response)
  - timing requirements (e.g. command rate, maximum delay time, and maximum time jitter for sampling rate and delay)
  - maximum allowed noise, including quantization noise from D/A conversion (RMS, PSD)
  - FDIR requirements
- Operational requirements
  - 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
- Configuration requirements
  - accommodation requirements (e.g. position and orientation of actuator)
  - avoidance of disturbances caused by actuator

- Interface requirements
  - alignment requirements (bias and stability)
  - electrical interface requirement (e.g. maximum noise for analogue interfaces)
  - data interface requirement (e.g. resolution)
- Verification requirements
  - testing interface requirements (stimuli outputs)
  - special provisions for ground testing

All properties of the actuators can be checked for feasibility.

#### 5.2.3.3 Controller hardware requirements

The following requirements for the controller hardware can be defined:

- sampling rates for sensor reading
- sampling rates for actuator commanding
- sampling rates for controller functions
- allowed processing delays for reading sensor information, controller processing and actuator commanding
- allowed time jitter in delays
- electrical interface requirements (including requirements for anti-aliasing filters)
- 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.

All properties of the controller hardware can be checked for feasibility.

#### 5.2.3.4 Controller software requirements

The following requirements for the controller software can be defined:

- algorithms for all “classical” control functions (see Figure 4-2) to be implemented in the controller
  - definition of desired state
  - determination of estimated state
  - derivation of control commands
- algorithms for all other control functions
  - control mode management
  - control system status monitoring
  - failure detection, isolation and recovery
- precision for the calculation of the control algorithms

- control software timing conditions (sampling rates, delays and jitter) in a consistent way together with the controller hardware timing conditions
- requirements for safety critical control functions
- control S/W interface requirements
  - from-to sensors and actuators
  - from-to system level control (on-board or ground)

All properties of the controller software can be checked for feasibility.

### 5.2.4 Control verification requirements

Control engineering identifies and defines 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

Control engineering specifies the modes and mode transitions. For each mode, control engineering defines how the control functions are allocated, e.g. control between hardware-software-human operations, and between on-board and on-ground.

Control engineering defines typically:

- the control operator interface requirements (e.g. specified MMI functions and processing requirements),
- the telemetry data needs from control point of view,
- the calibration process and the ground software requirements,
- 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

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

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

Analysis contributes to the whole control engineering process, as depicted in Figure 4-3. In line with ECSS-E-ST-10, the analysis process interacts strongly with all the other control engineering activities.

Within control engineering, the objects of the analysis are the controller, the sensors and actuators, the controlled plant, and the external environment (see Figure 4-1). 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

For all control engineering functions, analytical methods and tools are used and properly adapted to each analysis task (per project phase). A list of usual analysis methods and tools is summarized in Table 5-1.

**Table 5-1: Contributions of analysis to the CE process**

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

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

Analysis is also based on the use of validated methods and tools, of demonstrable adequacy for this task.. In case of new tool development, control engineering contributes to the specification, development and validation of such tool, managed as part of the control engineering process.

The selected tools are identified and documented in terms of type of tool, version, implemented methods, and platform (H/W and operating system). Particular attention should be given to:

- compatibility for data exchange with tools used by other engineering domains,
- portability across different platforms.

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

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

### 5.3.3 Requirements analysis

In the framework of the requirements engineering process, 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 4-1;
- definition of human-in-the-loop constraints.

For each phase defined in Table 4-2 to Table 4-5, requirements analysis results in a detailed control error budget to be used as input for the technical specification of control components.

Analysis supports 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).

Analysis assesses feasibility of requirements allocated to the different control components.

### 5.3.4 Disturbance analysis

Disturbance analysis covers all mission scenarios, over the whole mission lifetime of the controlled system. Control engineering performs the analysis to define the internal and external disturbances to the controlled system as defined in Figure 4-1:

- Disturbances originating in the plant are defined based on the system requirements;
- External disturbances due to the space environment are identified (for space environment, see ECSS-E-ST-10-04).

Usage of different models (e.g. for special applications analysis) are justified, and agreed with the customer on a case-by-case basis.

Internal disturbances (e.g. actuator vibration, friction, and noise) are modelled using verified parameters (e.g. manufacturer data) or parameters identified by dedicated tests. Worst case parameters can be used to avoid tests provided that robustness is demonstrated w.r.t these parameters.

### 5.3.5 Performance analysis

Performance analysis is conducted during all the phases of the control development process. It assesses that the controlled system performance is coherent with

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

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

For performance analysis, mathematical models are developed and used. The number and detail of the models depend on the project phase.

#### 5.3.5.1 Early phases models

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

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

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

#### 5.3.5.2 Phase C/D models

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

The mathematical models used for detailed simulations of the controlled system includes:

- Model of the controlled plant:
  - — dynamics,
  - — kinematics (coordinate transformations).
- Models of the sensors.

- Models of the actuators.
- Model of the controller hardware:
    - timing conditions,
    - A/D and D/A quantization.
- Model of the controller functions (controller software):
    - control algorithms, with representative timing and numerical precision control algorithms;
    - interface to system level control, like e.g. reference signals (reference state), or mode switching commands.
- Model of the relevant disturbance sources:
    - internal disturbance sources (within the controlled system), which can be part of the sensor, actuator, controller or plant models;
    - external disturbance sources (from the environment), which can be part of the sensor, actuator, controller or plant models.
- Model of the environment (for modelling the control relevant influences onto the controlled system):
    - nominal inputs (e.g. Sun position as input to sun sensor),
    - external disturbances sources.
- Model of the control signals interfaces, like e.g. timing conditions, or noise (for analogue interfaces).

#### 5.3.5.3 Features and usages of mathematical models

The models defined are calculated with a numerical precision in line with the control problem. 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).

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

- direct evaluation of the outputs in the time domain, and
- input-output data post-processing.

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

- assessment of fulfilment of control objectives;
- sensitivity analyses for design trade-offs and optimization of product selection;
- sensitivity analyses for assessment of control design robustness (against variations and uncertainties in the controlled system parameters).

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

- time domain requirements such as:
  - response to reference signals (e.g. response time, settling time, and tracking error for command profiles);
  - accuracy and stability errors in the presence of disturbances;
  - measurement errors (e.g. attitude knowledge).
- frequency domain requirements (e.g. bandwidth).

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

#### 5.3.5.4 Relationship with budgets

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

The performance analysis supports the maintenance of control budgets throughout the control engineering process.

The value used for each contributor is 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 can be 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

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.

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

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

### 5.4.3 Operational design

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.

Control engineering defines 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.

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

The operational control architecture is usually presented in the form of diagrams showing control modes, transitions and data flows:

- For each control mode, the design identifies
    - the functions involved,
    - the allocation of functions to H/W, S/W and humans,
    - the allocation of functions to ground and on-board,
    - the conditions of validity of the control mode, and
    - its contribution to the control objectives.
- For each transition; the design also identifies
    - starting conditions (previous mode and specific conditions),
    - when the transition occurs (trigger conditions),
    - end-conditions (subsequent mode and specific conditions),
    - functions to be performed during the transitions.

### 5.4.4 Control implementation architecture

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. More specifically, control engineering contributes or is involved in the following activities:

- definition of a set of requirements for sensors which can meet all the control objectives in terms of performance, redundancy, observability and operability;

- definition of a set of requirements for actuators which can meet all the control objectives in terms of controllability, performances and redundancy;
- checking if the operational dynamic conditions of plant are compatible with the selected configuration of sensors and actuators;
- contribution to the design of the plant with respect to the system dynamics and kinematics affecting the control performance;
- verification that the selected plant physical configuration is compatible with the control system design;
- contribution to the design of the electrical system architecture w.r.t. electrical interfaces affecting the control performance;
- contribution to the on-board processing architecture w.r.t processing capability, data rates, inputs-outputs, memory affecting the control performance;
- verification 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;
- verification 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

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

### 5.4.5.1 Nominal design

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

The control algorithms are designed to be compatible with operational requirements such as

- autonomy with respect to the ground;
- observability from the ground;
- delay in ground reaction due to transmission delays or availability of ground equipment or operators;
- capability for in-flight reprogramming by uploading the S/W patches.

### 5.4.5.2 Robustness to uncertainties or evolutions

The controller is designed to achieve the control objectives while being robust to uncertainties or predicted evolutions in the controlled system (controlled plant or control components). 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.

#### 5.4.5.3 Robustness to failures

The controller is designed to react to possible (expected) failures in the control system components or the plant. A set of potential failures is defined in agreement with the system engineering) in order to:

- enable detection and identification of those failures either autonomously or from the ground;
- enable a recovery after occurrence of those failures (no loss of mission);
- meet the performance specified after the occurrence of those failures.

## 5.5 Verification and validation

The control engineering verification and validation process is a part of the system verification and validation process.

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.

### 5.5.1 Definition of control verification strategy

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

- verifies that the controlled system is capable of achieving the specified control objectives;
- verifies the design and performance of each part of the control system with respect to the allocated requirements;
- verifies that the flight hardware and software components of the control system conform to the requirements and are acceptable for use;
- confirms controlled system integrity and performances after specified steps of the project life cycle (e.g. pre-launch and in-flight).

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

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

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

- a description of the control engineering verification and validation tasks;
- the resources, responsibilities and schedule;
- a description of the procedures, tools and facilities used for verification, including the way they are themselves validated;
- the model philosophy.

The different control engineering verification tasks are 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 Preliminary verification of performance

To reduce risks, the control verification process starts early in the project to validate the control concepts and design as they become available. This process is often iterative according to the design maturity.

The verification of critical features is performed during the design and development phases, relying on simulation models or development models (prototypes). The representativity and accuracy of the simulation models and tools used for the verification is assessed.

## 5.5.3 Final functional and performance verification

### 5.5.3.1 Verification by analysis

The performance of the controlled system is demonstrated by closed-loop analysis based on the use of system representative simulation models. The verification covers all operational configurations of control modes and sensors-actuators, including back-up configurations. Worst cases conditions are generally used w.r.t system dynamical and geometrical configurations, including FDIR aspects and associated possible degraded configurations.

When relevant or possible, verification by analysis is supported by H/W testing. A typical example is to correlate a sensor mathematical model, including its parameters, with H/W tests results.

### 5.5.3.2 Verification with flight H/W and S/W

The control verification process includes, when relevant, functional validation in closed-loop tests with flight S/W and flight H/W models or flight representative models. The real sensors are stimulated by the EGSE. The stimuli can be electrical (test connector) or physical (detector level). The following aspects are verified:

- Function and performance of the flight hardware components of the control system;
- Numerical accuracy of the control S/W on the target H/W (or emulator). This numerical accuracy can be verified by hardware-in-the-loop tests or comparison with numerical simulations;
- Mode transitions including FDIR mechanisms;
- polarity of the sensors and actuators (after final integration).

## 5.5.4 In-flight validation

When in-flight validation is specified, the necessary observability of the controlled system is provided through the ground segment.