

Title: **ECSS-E60 Control Engineering Standard**

Author: E60 Working Group Members..... Date: 28.11.01

Checked by: E60 Working Group Members..... Date: 28.11.01

Distribution List

| Name | Company | Copies |
|--|--|--------|
| Jacques Dumanchin | Aerospatiale-Matra (L1 Engineering WG) | 1 |
| Joerg Flemmig | Astrium GmbH, Friedrichshafen | 1 |
| David Soo | ESA/ESTEC | 1 |
| Donato Sciacovelli | ESA/ESTEC | 1 |
| Peter Putz | ESA/ESTEC | 1 |
| Philippe Marchal, Paola Van-Troostenberghe | CNES, Toulouse | 1 |
| Bruno Musetti | Alenia, Torino | 1 |
| Philippe Charbonnel | Alcatel, Cannes | 1 |
| Thierry Duhamel | Astrium SAS, Toulouse | 1 |
| Donato Borrelli | Officine Galileo, Firenze | 1 |
| Jan Kouwen | Fokker Space, Leiden | 1 |

Change Record

| Issue | Date | Pages | Change Description |
|--------------|------------|--|---|
| Draft | 22.09.1999 | all | First edition (table of contents) |
| Version 1 | 16.05.2000 | all | Draft contents of chapters 1 to 3, minor modifications of other chapters |
| Version 2 | 15.06.2000 | Section 1 Section 2 Section 3 Section 4 | First full text formulation of Introduction First Informative reference added Some definitions added Draft section 4 added |
| Version 3.0 | 11.07.2000 | all | Modifications during meeting #3 |
| Version 3.1 | 17.07.2000 | all | Minor updates (harmonisation of meeting #3 inputs) |
| Version 3.2 | 20.07.2000 | Sections 1 - 3 | Updates after meeting 3 |
| Version 3.3 | 01.08.2000 | Sections 3 & 4 | A few definitions added and §4 updated according to decisions of meeting 3. |
| Version 3.4 | 25.09.2000 | all | Editorial changes |
| Version 4.0 | 26.09.2000 | all | Changes agreed during meeting 4 |
| Version 4.1 | 13.11.2000 | Section 5 | Inclusion of draft inputs for section 5 |
| Version 5.0 | 14.11.2000 | all | Changes agreed during meeting 5 |
| Version 6.0 | 25.01.2001 | all | Changes agreed during meeting 6 |
| Version 6.1 | 29.01.2001 | Sections 4 & 5 | Editorial changes |
| Version 6.2 | 05.03.2001 | Sections 4 & 5 | Inclusions of inputs for section 5.2 and 5.3 |
| Version 7.0 | 08.03.2001 | all | Changes agreed during meeting 7 |
| Version 8.0 | 18.04.2001 | Section 5 | Changes agreed during meeting 8 |
| Version 8.1 | 23.05.2001 | Section 5.2 | Inclusions of inputs for section 5.2 |
| Version 9.0 | 29.05.2001 | all | Changes agreed during meeting 9 |
| Version 10.0 | 10.07.2001 | Section 5 | Inclusion of new inputs for section 5.3 and 5.5, changes agreed during meeting 10 |

Table of Contents

| | |
|--|-----------|
| 1. Scope | 7 |
| 1.1 Introduction | 7 |
| 1.1.1 Purpose of the control engineering standard | 7 |
| 1.1.2 Scope of the control engineering standard | 7 |
| 1.1.2.1 The general control structure | 7 |
| 1.1.2.2 Control engineering tasks | 9 |
| 1.1.3 Organisation of this document | 10 |
| 1.2 Relationship with other standards | 10 |
| 1.2.1 ECSS engineering standards | 10 |
| 1.2.2 ECSS project management standards | 11 |
| 1.2.3 ECSS product assurance standards | 11 |
| 1.2.4 Non-ECSS standards | 11 |
| 2. Normative references | 12 |
| 3. Terms, definitions and abbreviations | 13 |
| 3.1 Terms and definitions | 13 |
| 3.2 Abbreviations | 18 |
| 4. Space control system engineering process | 19 |
| 4.1 Definition of the control engineering process | 19 |
| 4.2 Control engineering tasks per project phase | 21 |
| 5. Requirements on the control engineering process | 29 |
| 5.1 Integration and control | 29 |
| 5.1.1 Organisation and planning of control engineering activities | 29 |
| 5.1.2 Contribution to control system engineering database | 29 |
| 5.1.3 Management of I/Fs with other disciplines | 29 |
| 5.1.4 Contribution to human factors engineering | 29 |
| 5.1.5 Definition of budget and margin philosophy for control | 30 |
| 5.1.6 Assessment of control technology and cost effectiveness | 30 |
| 5.1.7 Risk management | 30 |
| 5.1.8 Engineering support to control components procurement | 30 |
| 5.1.9 Support to change management involving control | 30 |
| 5.1.10 Control engineering capability assessment and resource management | 30 |
| 5.2 Requirements engineering | 31 |
| 5.2.1 Generation of control requirements from system requirements | 31 |
| 5.2.2 Contribution to system requirements to meet control requirements | 31 |
| 5.2.3 Allocation of control requirements to control components | 32 |
| 5.2.3.1 Sensors | 32 |
| 5.2.3.2 Actuators | 32 |
| 5.2.3.3 Controller hardware requirements | 33 |

| | | |
|---|--|-----------|
| 5.2.3.4 | Controller software requirements | 33 |
| 5.2.3.5 | Control components interface requirements..... | 34 |
| 5.2.4 | Control verification requirements..... | 34 |
| 5.2.5 | Control operations requirements | 34 |
| 5.3 | Analysis | 35 |
| 5.3.1 | Contribution of the analysis to control engineering process..... | 35 |
| 5.3.2 | Performance analysis..... | 37 |
| 5.3.3 | Trade studies | 38 |
| 5.3.4 | Analysis tools and methods | 39 |
| 5.3.5 | Analysis of requirements..... | 40 |
| 5.3.6 | Budgets methods and margins..... | 40 |
| 5.4 | Design and configuration | 41 |
| 5.4.1 | Functional design..... | 41 |
| 5.4.2 | Physical control architecture | 44 |
| 5.4.3 | Controller design..... | 45 |
| 5.4.4 | Configuration management and controller budgets | 45 |
| 5.4.5 | Other topics | 46 |
| 5.5 | Verification and validation | 46 |
| 5.5.1 | Definition of control verification strategy | 46 |
| 5.5.2 | Preliminary verification of performance | 47 |
| 5.5.3 | Final functional & performance verification..... | 47 |
| 5.5.3.1 | Verification by analysis | 47 |
| 5.5.3.2 | Verification with flight H/W and S/W..... | 48 |
| 5.5.3.3 | Acceptance verification (to be checked with 5.5.3.1 and 5.5.3.2) | 48 |
| 5.5.4 | In orbit validation..... | 48 |
| 5.6 | Operations | 49 |
| Annexes: Document Requirements Definitions (DRD) | | 50 |

List of Figures

| | |
|--|----|
| Figure 1-1: General Control Structure | 8 |
| Figure 5-1: Analysis Contributions to the CE Process | 37 |

List of Tables

| | |
|---|----|
| Table 4-1: Summary of Control Engineering Activities | 20 |
| Table 4-2: Control Engineering Inputs, Activities and Outputs – Phase 0/A | 22 |
| Table 4-3: Control Engineering Inputs, Activities and Outputs – Phase B | 25 |
| Table 4-4: Control Engineering Inputs, Activities and Outputs – Phase C/D..... | 26 |
| Table 4-5: Control Engineering Inputs, Activities and Outputs – Phase E/F | 27 |
| Table 5-1: Contributions of Analysis to the CE Process | 36 |

1. Scope

1.1 Introduction

1.1.1 Purpose of the control engineering standard

Control engineering in general and particularly as applied to space systems is a highly multi-disciplinary field. The analysis, design and implementation of more complex (end-to-end) control systems have important aspects of system engineering, electrical and electronic engineering, mechanical engineering, software engineering, communications, ground systems and operations – all of which have their own dedicated ECSS engineering standards. For the relevant aspects, these standards shall apply and the Control Engineering Standard does not intend to duplicate them.

The Control Engineering Standard will, however, focus on the specific issues involved in control engineering and is primarily meant as a structured set of systematic engineering guidelines, making reference to the discipline specific standards where appropriate. For this and other important reasons (e.g. the very rapid progress of control component technologies and associated “de facto” standards), the Control Engineering Standard will 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 has been intentionally avoided. The readers and users of the standard are assumed to possess general knowledge of control systems engineering and its applications to space missions.

1.1.2 Scope of the control engineering standard

This standard concerns control systems developed as part of a space project. It is potentially 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, which are addressed in the Management (-M) and Product Assurance (-P) branches of the ECSS System, and explains how they apply to the control engineering process.

1.1.2.1 The general control structure

To illustrate and delineate the scope of control engineering, consider Figure 1-1 which shows a general control structure. This fundamental diagram allows to introduce the following basic concepts and definitions:

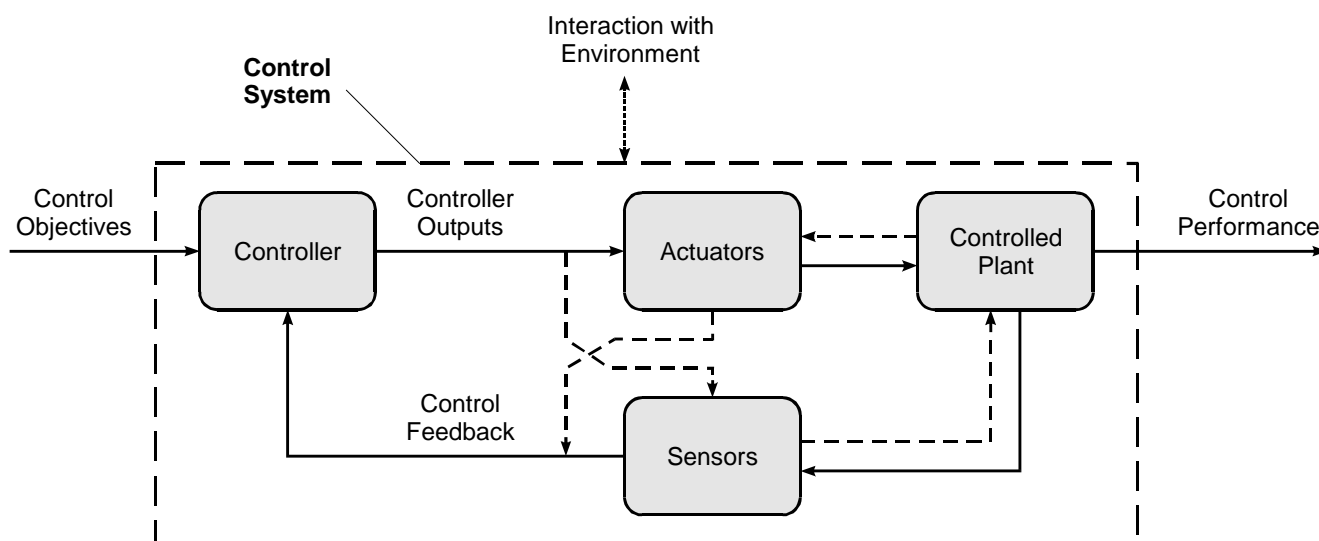


Figure 1-1: General Control Structure

The control system is defined as the control relevant part of a system which has to achieve the required control objectives. It includes all relevant functional behaviour of controllers, sensors, actuators and plant.

Control engineering always concerns some feedback loop. There is a physical system whose intrinsic behaviour and output need to be modified and shaped (improved in the sense of some well-defined objectives). We call this the Controlled Plant. For space applications, the Controlled Plant can be

- ☐ a satellite (w.r.t. its attitude and orbit, or w.r.t. to its temperatures in the case of active thermal control, etc.) 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
- ☐ etc.

The users of the Controlled Plant pursue very specific goals. At the most abstract level, we call these Control Objectives. The purpose is to have a Controller which gives the Controlled Plant a desired Control Performance, despite its interaction with its Environment.

To do this, suitable technical interfaces have to be present: Actuators which can convert controller outputs 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 inputs to the Controller.

Besides this primary flow of information which forms a classical feedback loop, the dashed arrows in Figure 1-1 also show some secondary flow of information or physical reaction. With more complex plants, Sensors and Actuators can be quite complex systems of their own with additional cross-

coupling of information, e.g. Controller Outputs can modify the configuration or parameters of a Sensor, or Actuators can produce direct feedback to the Controller. The dynamics of the Controlled Plant may have a relevant physical effect on the Actuators and Sensors, and the operation of the Sensors may feed back onto the Controlled Plant.

Control Objectives (as the command 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 control system will consist of many layers of (typically hierarchically decomposed and refined) Controllers and their Controlled Plants (which may be suitable abstractions of lower level control loops).

Consequently, also the Control Performance can 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 of its own right. In the most general case, we consider the Controller 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 ground)
- ❑ aspects of planning (quasi “off-line” preparation of the commands to give in the future) and of execution of these commands (“on-line” in the sense of the update frequency of the control loop)
- ❑ nominal and **backup** control (exception handling, failure detection, isolation and recovery, ...)

This notion of controller generality is a powerful concept which – among others – allows a quite natural definition of the various Degrees of Autonomy or “intelligence” which 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 will be based on a judicious trade-off considering aspects like predictability of the situation (availability of reliable models), required reaction time, available on-board computer resources, available telecommunications coverage and bandwidth, decision-making complexity, cost of development and operations, acceptable risk, etc.

The consideration of human operations and ground systems in the control engineering process should not be 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 the Control Engineering Standard will make due reference to the applicable Standard E70 (“Ground Systems and Operation”).

1.1.2.2 Control engineering tasks

From the general control structure introduced above, it becomes clear that control engineering has to include at least

- ❑ 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.

This shows that control engineering

- ❑ is quite multi-disciplinary (requiring 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 interaction with the system engineering process specified in the E-10 standard.

1.1.3 Organisation of this document

To be reviewed and adapted to final structure / contents !!

This standard is organised as follows:

- ❑ Section 4 sets the framework for the control engineering process. The main engineering functions are defined and characterised by their inputs, internal sub-processes, outputs (incl. documents), typical milestones, and relationship to the typical project phases.
- ❑ Section 5 treats each of these engineering functions in detail, specifying their main activities and expected outputs. These are the core normative requirements for control engineering in general space systems.
- ❑ Section **Error! Reference source not found.** contains additional discipline-specific requirements. These are considered applicable for their respective Applications only (e.g. control of pointing systems, of space robot systems, thermal control)
- ❑ The Annexes give the required structure and contents of the key documents to be produced in the control engineering process.

1.2 Relationship with other standards

This Section discusses how this standard interfaces with other ECSS standards and points out relations to non-ECSS standards.

1.2.1 ECSS engineering standards

- ❑ ECSS-E-00 "Policy and Principles" 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 the Control Engineering Standard.
- ❑ ECSS-E-10 "System Engineering" defines requirements for space system engineering. Because of the significant system aspect of control engineering, E-10 is therefore particularly applicable and important.

- ❑ Because of the multi-disciplinary character of control engineering, all the parallel Level 2 engineering standards are applicable for details in the disciplines of electrical and electronic engineering (E-20), mechanical engineering (E-30), software engineering (E-40) communications (E-50), ground systems and operations (E-70). Where control specific issues are concerned, however, the Control Engineering Standard (E-60) takes precedence.

1.2.2 ECSS project management standards

The ECSS M standards define the requirements to be applied to the management of space projects. Of particular relevance are

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

1.2.3 ECSS product assurance standards

The ECSS Q series of standards define the requirements to be applied to product assurance of space projects.

???? anything in particular ???

1.2.4 Non-ECSS standards

e.g. AIAA, ISO

??? what do we write here ??

2. Normative references

❑ analogous as other standard

❑ applicable documents/standards

| | |
|-----------------|---|
| ECSS-P-001 | Glossary of Terms |
| ECSS-E-00 | Space engineering – Policy and principles |
| ECSS-E-10 | Space engineering – System engineering |
| ECSS-E-20 | Space engineering – Electrical and electronics |
| ECSS-E-30 | Space engineering – Mechanical |
| | – Part 1: Thermal control |
| | – Part 2: Structures |
| | – Part 3: Mechanisms |
| | – Part 5: Propulsion |
| ECSS-E-40 | Space engineering – Software |
| ECSS-E-50 | Space engineering – Communications |
| ECSS-E-70 | Space engineering – Ground systems and operations |
| ECSS-M-00 | Space project management – Policy and principles |
| ECSS-M-10 | Space project management – Project breakdown structures |
| ECSS-M-20 | Space project management – Project organisation |
| ECSS-M-30 | Space project management – Project phasing and planning |
| ECSS-M-40 | Space project management – Configuration management |
| ECSS-M-50 | Space project management – Information/documentation |
| ECSS-M-60 | Space project management – Cost and schedule management |
| ECSS-M-70 (TBC) | Space project management – Integrated logistics support |
| ECSS-Q-20 | Space product assurance – Quality assurance |

Level 3 documents referenced by this standard:

| | |
|-------------|------------------------------------|
| ECSS-E60-01 | ESA Pointing Budget Error Handbook |
|-------------|------------------------------------|

3. Terms, definitions and abbreviations

3.1 Terms and definitions

This Section contains terms for which the ECSS-P-001 definitions have been further expanded to cover control specific issues, and additional terms which are essential for a systematic definition and common understanding of the control engineering process and requirements.

Keywords (terms which are to be used in the particular meaning of these definitions) are capitalised throughout the text of this standard (e.g. "Operation" with specific meaning as opposed to "operation" with general meaning).

Absolute Pointing Error

Absolute Rate Error

Actuator

A technical system or device which converts commands from the Controller into physical effects on the Controlled Plant.

Algorithm

Aliasing

Analysis

The determination of the essential qualities, performances and limitations of an item by cognitive or computational methods.

Application

The particular use specified for a Controller in a certain mission. This comprises both the Mission Objectives and the actual space system (Controlled Plant) chosen a priori for that purpose. The application says FOR WHAT the control functions have to be performed.

Attitude Control Cycle

Attitude Sensor Errors

Autonomy, Degree of Autonomy

Autonomy is the capability of a system to perform its functions in the absence of certain resources. Since there is an enormous variety of functions and resources, autonomy as such is an ill-defined concept. 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 segment / ground segment, and preparation / execution. A low Degree of Autonomy will be characterised by few functions performed in software in the space segment. Conversely, a high

Degree of Autonomy will assign 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 the amount of “machine intelligence” installed in the system.

Bandwidth**Bang-Bang****Bending Mode****Bias****Control (as in GNC)****Control component**

An element of the (controlled) system which is used in part or in total to achieve control objectives.

Control Mode**Control Stability****Controllability****Control system**

The control system is defined as the control relevant part of a system which has to achieve the required control objectives. It includes all relevant functional behaviour of controllers, sensors, actuators and plant.

Control Objectives

The Control Objectives specify the goal of the control problem. They are issued as commands to the Controller, which then has to give the Controlled Plant a desired 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.

Control Performance

The Control Performance is the useable output generated by the Controlled Plant. It is achieved by the Controller through Sensors and Actuators.

Controlled Plant

The Controlled Plant is the (part of a) physical system which is the target of the control problem. The purpose is to modify and shape the intrinsic behaviour of the Controlled 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, etc.

Control Task:

subset of control objectives

Controller

A Controller is a system designed to give the Controlled Plant a desired Control Performance. It 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.

Damping Factor**Dead-Band****Degree of Autonomy**

see Autonomy

Describing Function**Discrete/Continuous Control****Disturbance****Drift****Environment****Estimator****Feed-Back****Feed-Forward****Filter****Function**

Description of a job or duty to be performed, preferably in terms of its input information, boundary conditions, and expected output. Graphically represented by a box or bubble with arrows indicating the information interfaces. A Function states WHAT has to be done, strictly independent of HOW and BY WHOM it may be performed (see also Application, Implementation, Operation).

Functional Control Architecture

Functional Layer

A main functional module resulting from a hierarchical decomposition of the overall Controller functionality. Functions on the same Functional Layer share important properties such as complexity of scope, functional abstraction, fundamental bandwidth of input or output command update.

Gain Margin**Guidance (as in GNC)****Implementation**

The actual technological solution in selection, allocation, and configurations of methods (algorithms), computer hardware, software, or human operations (Brainware) that is chosen for a specific realisation and for a specific Application to carry into effect a certain Function. The Implementation says HOW a Function is performed.

- ☐ Jitter
- ☐ Limit Cycle
- ☐ Linear/Non-Linear Systems
- ☐ Mapping

Navigation (as in GNC)**Noise****Noise Equivalent Angle****Nutation****Observability****Operation**

A mode of Operation describes the circumstantial fashion (mostly w.r.t. the extent of human involvement) in which particular Functions are to be performed. For instance, the mode of Operation specifies the allocation of control Functions among humans (Brainware) and machines (hardware and software) of different specialisation and skill level and at different sites (e.g. in the Ground Segment or in the Space Segment). The mode of Operation says BY WHOM a Function is performed, but not HOW (see Implementation).

Orbit Control**Passive/Active Control****Phase Margin**

Pointing Accuracy

Pointing Drift

Pointing Knowledge (Attitude Determination Accuracy)

Pointing Stability

Power Spectral Density

Precession

Quantisation

Quaternion

Random Walk

Rate Measurement Error

Regulator

Relative Pointing Error

Robustness

Sampling

Sensor

A Sensor measures states of the Controlled Plant and provides them as feedback inputs to the Controller.

Skewed

State

State Diagrams

Steering

Sub-assembly

An ensemble of control components e.g. the attitude measurement sub-assembly.

Systematic Error

Target

Tracking

Transducer

Unpredictable Error

Verification

See E10

Validation

See E10 ?

3.2 Abbreviations

- ☐ AOCS - attitude and orbit control system
- ☐ A&R - automation and robotics
- ☐ CE - control engineering
- ☐ GNC - guidance, navigation and control
- ☐ PSD - power spectral density
- ☐ LOS - line of sight
- ☐ TBD - to be defined
- ☐ w.r.t. - with respect to

4. Space control system engineering process

4.1 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-E10-A (the reader should refer to this standard for the definition of the System Engineering process). As such it can also be broken down into the same functions:

- ❑ Integration and Control, which ensures the integration of the various control related disciplines throughout all the project phases towards the total definition and realisation 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 assembly or equipment level requirements and continuous supervision of their status and traceability.
- ❑ Analyses, 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; 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, to demonstrate, through a dedicated process, that the system meets its control requirements.

These different control engineering functions need, at various stages of the controlled system development, to be conducted in parallel to support one another in the proper development of the controlled system and of its components.

Table 4-1 provides a summary of the specific Control Engineering activities corresponding to each function.

After the functional specification of the controlled system it is likely that hardware, software, 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 must be defined so as to allow these iterations.
- ❑ progressive from preliminary design to verification and in-orbit validation. The typical control engineering tasks, inputs and outputs according to the chronological phases of a programme are detailed in section 4.4.
- ❑ particularly iterative between requirements engineering, analysis and design/configuration.

| Control Engineering Functions | Specific Control Engineering Activities |
|-----------------------------------|---|
| Integration & Control | <ul style="list-style-type: none"> - organisation and planning of control engineering activities - contribution to control system engineering database - management of I/Fs with other disciplines (mechanical engineering, software engineering, etc.) and activities (procurement, quality assurance, etc.) - contribution to human factors engineering when control systems are involved - 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 - control engineering capability assessment and resource management |
| Requirements Engineering | <ul style="list-style-type: none"> - 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 | <ul style="list-style-type: none"> - selection of adequate and well accepted 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 program imposed constraints like cost, schedule and risk - numerical analysis to support the control design - performance verification analysis (including simulation) - numerical analysis to support in flight evaluation |
| Design & Configuration | <ul style="list-style-type: none"> - 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 - establish control budgets - contribution to selection and procurement of control components - contribution to system configuration management |
| Verification | <ul style="list-style-type: none"> - definition of control verification strategy - preliminary verification of performance by analysis or prototyping - final functional and performance verification by analysis - final verification/validation of control system (H/W, S/W and human operation) by test and hardware-in-the-loop simulations - in-orbit validation of control system behaviour |

Table 4-1: Summary of Control Engineering Activities

4.2 Control engineering tasks per project phase

This section describes in which detail the engineering tasks have to be performed in each phase of the project. Table 4-2 shows for each task the required input, the activities and the output.

| O/A | Integration & Control | Requirements Engineering | Analysis | Design & |
|-------------------|--|---|---|---|
| Inputs | <ul style="list-style-type: none"> - System development schedule - System development philosophy and constraints | <ul style="list-style-type: none"> - System objectives - Mission requirements - System pointing accuracy | - Control system objectives | |
| Activities | <ul style="list-style-type: none"> - First assessment of control system development cost and schedule - Generation of inputs to the system development philosophy - Identification of availability and maturity of control technology | <ul style="list-style-type: none"> - Translate mission and system objectives into preliminary control objectives - Definition of preliminary control requirements - Control system life cycle definition | <ul style="list-style-type: none"> - Analysis of control requirements feasibility for control system alternatives - Disturbances evaluation - Preliminary performance assessment - Initial control system sensitivity analysis - Identification of control system critical aspects | <ul style="list-style-type: none"> - Establishment of control concepts - Establishment of system de |
| Outputs | <ul style="list-style-type: none"> - Inputs to project and system engineering management plan - Inputs to cost estimates and schedule, cost and schedule estimates - Inputs to technology development plan | <ul style="list-style-type: none"> - Inputs to system requirements documentation | <ul style="list-style-type: none"> - Control system analyses (input to control design and analysis report) | <ul style="list-style-type: none"> - Preliminary and analy |

Table 4-2: Control Engineering Inputs, Activities and Outputs – P





| B | Integration & Control | Requirements Engineering | Analysis | Design & |
|-------------------|---|--|--|--|
| Inputs | <ul style="list-style-type: none"> - Phase 0/A project planning and cost estimates | <ul style="list-style-type: none"> - System objectives - Mission requirements - Control system requirements - Control life cycle phase 0/A | | |
| Activities | <ul style="list-style-type: none"> - Update control system inputs to system engineering management plan and cost estimates - Review of the control systems compatibility with the system design and constraints | <ul style="list-style-type: none"> - Analyse system requirements - Generate control system requirements - Allocate control system requirements to subsystems and components - Check traceability of control requirements with respect to system requirements | <ul style="list-style-type: none"> - Analysis of control requirements for sub-systems and components - Control system performance analysis - Analysis of control system sensitivity - Assessment of control system robustness against disturbances - Trade-off studies for supporting control system architecture definition - Assessment of control technologies for early prototyping - Establishment of control system budgets and margins | <ul style="list-style-type: none"> - Definition baseline - Allocation functions to human operator on ground - Definition interfaces - Preliminary controller - Definition FDIR - Selection of component - Establishment of system budgets and margins |
| Outputs | <ul style="list-style-type: none"> - Inputs to project and system engineering management plan - Inputs to cost estimates and schedule | <ul style="list-style-type: none"> - Inputs to system or subsystem technical specifications - Inputs to lower level technical specifications - Inputs to requirements database - Inputs to interface control documents | <ul style="list-style-type: none"> - Control system analysis report (including simulation models description) | <ul style="list-style-type: none"> - Control system report - Preliminary algorithms - Preliminary budgets |



Table 4-3: Control Engineering Inputs, Activities and Outputs – F

| C/D | Integration & Control | Requirements Engineering | Analysis | Design & |
|-------------------|--|---|---|---|
| Inputs | <ul style="list-style-type: none"> - Phase B project planning and cost estimates | <ul style="list-style-type: none"> - Control life cycle phase B - Phase B design justification | <ul style="list-style-type: none"> - Control system objectives | |
| Activities | <ul style="list-style-type: none"> - Support of system engineering and project management - Management of required control system changes - Support of operations - Review of data packages - Support to phase E/F planning and cost estimate | <ul style="list-style-type: none"> - Update of specifications - Review and assessment of control requirements changes | <ul style="list-style-type: none"> - Detailed control system performance analysis - Update of control system sensitivity analysis - Detailed assessment of control system robustness against disturbances - Update of control system budget and margins | <ul style="list-style-type: none"> - Update of baseline - Finalisation of system functional architecture - Detailed design of controllers - Review of and margins |
| Outputs | <ul style="list-style-type: none"> - Updated inputs to project and system engineering management plan - Inputs to system database - Inputs to operations handbook/user manual - Updated cost estimates for phase E/F | <ul style="list-style-type: none"> - Updated inputs to system or subsystem technical specifications - Updated inputs to lower level technical specifications - Updated inputs to interface control documents | <ul style="list-style-type: none"> - Control system analysis report | <ul style="list-style-type: none"> - Final control report - Final control specifications - Final control system specifications - Final control budgets |

Table 4-4: Control Engineering Inputs, Activities and Outputs – PI



| E/F | Integration & Control | Requirements Engineering | Analysis | Design & |
|-------------------|---|---|---|----------------------------------|
| Inputs | - System operations planning | - Design reports | - control system in flight performance data | |
| Activities | <ul style="list-style-type: none"> - Support of system operations - Management of required controller changes - Control engineering support to system disposal - Generation of lessons learnt for control engineering | - Record control requirement feed-backs from control system performance | <ul style="list-style-type: none"> - Analysis of control system operational performance - Analysis of required controller changes | - Update of (in case of changes) |
| Outputs | - Inputs to disposal plan | | <ul style="list-style-type: none"> - Control system operational performance report - Inputs to payload data evaluation | |

Table 4-5: Control Engineering Inputs, Activities and Outputs – P

5. Requirements on the control engineering process

5.1 Integration and control

The Integration and Control function contributes to the System Engineering Integration and Control from a control point of view and consequently supports all system engineering management activities where control is involved or impacted.

Integration and Control shall, in particular, be consistent with the System Engineering Management Plan and System Engineering Integration and Control requirements as defined in ECSS-10-A.

5.1.1 Organisation and planning of control engineering activities

- 5.1-1: Control engineering shall contribute to the system engineering management plan to define, organise and plan all control engineering activities required to achieve the specified control performance. This applies especially for the control development and verification logic which is closely related to the system design and development planning.
- 5.1-2: Control engineering shall contribute and participate in all project reviews which are relevant for control.

5.1.2 Contribution to control system engineering database

- 5.1-3: Control engineering shall provide inputs to the system engineering database concerning controller parameters.
- 5.1-4: Control engineering shall provide inputs to the system engineering database w.r.t. control related actuator/sensor parameters (e.g. flight dynamics data base)

5.1.3 Management of I/Fs with other disciplines

- 5.1-5: Control engineering shall provide inputs and review related interfaces/disciplines, e.g.
 - electrical interfaces (noise, quantisation, sampling, timing)
 - mechanical interfaces (alignment, stiffness, eigenfrequencies, microvibrations)
 - thermal interfaces
 - software interfaces (control functions realised by S/W)

5.1.4 Contribution to human factors engineering

- 5.1-6: Control engineering shall contribute to human factors engineering in the case when humans are part of the control loop. The following factors have to be considered:
 - human performance capabilities
 - human/machine interfaces
 - training of control operators

5.1.5 Definition of budget and margin philosophy for control

- 5.1-7: The control related budgets and performance margins shall be clearly defined and shall be put under configuration control.

5.1.6 Assessment of control technology and cost effectiveness

- 5.1-8: The programmatic risk w.r.t. the maturity of the control related technology shall be analysed and assessed. This shall be done for
controller (H/W – S/W – human, analog/digital, ...)
sensors/actuators
- 5.1-9: The effort for the verifications of the control objectives shall be assessed.

5.1.7 Risk management

- 5.1-10: Control engineering shall contribute to risk analysis from a technical point of view
- 5.1-11: Control engineering shall support the FMECA by analysis of control loop behaviour in case of failures.

5.1.8 Engineering support to control components procurement

- 5.1-12: Control engineering shall support the system engineering for the procurement of the controller H/W and S/W.
- 5.1-13: Control engineering shall support the system engineering for the procurement of sensors/actuators.

5.1.9 Support to change management involving control

- 5.1-14: Control engineering shall support the management of non-conformances related to control.
- 5.1-15: Control engineering shall be responsible to handle changes related to controller design and implementation.
- 5.1-16: Control engineering shall review changes in control related disciplines.

5.1.10 Control engineering capability assessment and resource management

- 5.1-17: Control engineering shall assess the control related capability and experience.
- 5.1-18: Control engineering shall perform the related resource management w.r.t.
human resources
tools.

5.2 Requirements engineering

Control requirements, to be addressed by Control Engineering, can be of two types:

- ❑ requirements to be met by the control system. These control system requirements are derived from the system level objectives and broken down to
 - requirements onto the controller (as defined in section 1.1.2.1)
 - requirements onto sensors and actuators
 - requirements onto the plant (e.g. free field of view or inertia requirements)

The requirements can originate from the required control system objectives or from other constraints (e.g. control system verification).

- ❑ requirements or constraints the control system puts on operations

5.2.1 Generation of control requirements from system requirements

- 5.2-1: The control system requirements shall be derived from the directly applicable system requirements.
- 5.2-2: The control requirements engineering shall consider relevant constraints imposed by other system requirements (electrical power, mechanical configuration, thermal conditions, operations, etc.).
- 5.2-3: The control systems requirement shall be allocated to low level requirements for the control components (controller, sensors, actuators). This is supported by
 - analyses (budget oriented, simulation, ...)
 - tests (e.g. on existing equipment or breadboards), if necessary

Note: The allocation of low level requirements is usually an iterative process.
- 5.2-4: The control requirements engineering shall keep clear traceability and justification of the control requirements. This shall be in line with system requirements engineering process.
- 5.2-5: The control requirements engineering shall take into account system FDIR principles and failure management definitions.

5.2.2 Contribution to system requirements to meet control requirements

- 5.2-6: CE 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.
- 5.2-7: Through an appropriate document (ICD or database), the CE 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 (FOV, axis-alignments, mechanical setup (stiffness, eigenfrequencies, ...)).

5.2.3 Allocation of control requirements to control components

The analyst shall identify for any assembly or equipment the hereunder requirement if necessary according to the phase of the project.

discussed up to here (18.04.01)

5.2.3.1 Sensors

5.2-8: The following sensor properties shall be defined as part of the control system design (if applicable):

Work range (including limitations by operating conditions)

Resolution

Linearity

Absolute accuracy (after calibration)

Sampling rate of the readout (in Hz)

Maximum delay time between actual situation in the environment and readout by sampling

Maximum allowed jitter in sampling time and delay

Maximum allowed noise (including quantisation noise from A/D conversion)

Short term drift in accuracy

Long term drift in accuracy

Maximum allowed unpredictable bias

Measurement mode, e.g. "fine mode" or "coarse mode" (all of the above parameters may be specified separately for the different modes)

Calibration needs: type (permanent or occasional), frequency, duration, ground or on-board...

Failure management: kind of failures to monitor, kind of algorithms to apply, delays for reconfiguration, H/W and/or S/W health and status needs

5.2-9: Properties should be checked on feasibility.

5.2.3.2 Actuators

5.2-10: The following actuator properties shall be defined as part of the control system design:

Command rate

Response time after receiving (step) command.

Maximum allowed jitter due to processing delay, part of response time.

Work range(s) for actuating and speed.

Resolution, quantization

Linearity

Absolute accuracy (after calibration)

Short term drift in accuracy

Long term drift in accuracy

Response time and settling times shall be clearly defined: time needed to achieve certain accuracy after (step) command

Utilisation mode : e.g. torque or speed control, sampled or continuous

Calibration needs : type (permanent or seasonal), frequency, duration, ground or on-board, parameters to refresh...

Failure management : what kind of failure to monitor, what kind of algorithms to apply, what delays for reconfiguration or more

H/W and/or S/W status needs

Electrical interface requirement

5.2.3.3 Controller hardware requirements

5.2-11: The following properties of the controller (processor) shall be defined as part of the controlled system design:

Sampling rates of reading sensors

Sampling rates of commanding actuators

Sampling rates of controller activities

Allowed processing delays for reading sensor information, controller processing and sending commands

Allowed jitter in delays

Information about complexity of algorithms as input for code sizing and processing load assessment

Electrical interface requirement

5.2.3.4 Controller software requirements

5.2-12: *The control engineering shall define algorithms for attitude estimation*

5.2-13: *The control engineering shall define algorithms for control laws calculation*

5.2-14: *The control engineering shall define sampling rate or timing of calculation and allowable related jitter*

5.2-15: *The control engineering shall identify any S/W status for nominal and failed functioning of the control*

5.2-16: *The control engineering shall identify suspendable and non suspendable processing*

5.2-17: *The control engineering shall define needs for segregating calculation activities*

versus failure process management

5.2-18: *The control engineering shall define the global failure management diagram*

5.2.3.5 Control components interface requirements

5.2-19: Internal interface issues :

timing of control signals between components

data format of control signals between components, *does this only cover sensor/actuator interface with on-board computer?*

5.2-20: External interface issue: *as it is the requirement phase for control, I don't see the content of this paragraph*

Operational use, restrictions

Environmental conditions

5.2.4 Control verification requirements

5.2-21: The control engineering shall identify the design requirements (e.g. test interfaces) to allow the verification process on all levels (component to control system level).

5.2.5 Control operations requirements

5.2-22: *The control engineering shall define the calibration process and the relevant ground software requirements.*

5.2-23: *The control engineering shall define the telemetry data needs from control point of view.*

5.2-24: *The control engineering shall define the failure management on ground with respect to the global ground system failure management.*

5.3 Analysis

Analysis is a fundamental activity that shall be performed at all levels of the control system, in all domains of control engineering and in all control modes for the purpose of:

- ☐ supporting in the allocation of requirements between control functions or physical components
- ☐ substantiating selection of control functional or physical architectures and implementations
- ☐ trading off alternative control solutions
- ☐ identifying design risk factors
- ☐ verifying the control system relative to its requirements
- ☐ assessing control performances

According to ECSS-E10, clause 1.1, see Figure 2, the analysis process is highly interacting with all the other Control Engineering functions. Furthermore, analysis shall be an iterative process.

Within the control system engineering framework the objects of the analysis shall be (see Figure 1-1) the controller, the sensors and actuators, the controlled plant, and the external environment. Such elements shall be processed by the analysis in order to assess the capacity of the control system of mapping the control objectives into control performance.

5.3.1 Contribution of the analysis to control engineering process

As shown in Table 5-1 analysis contributes to all the Control Engineering process. In the following each analysis contribution is described.

| Control Engineering Functions | Analysis Activities | Typical Methods and Tools |
|---------------------------------|---|--|
| Requirements Engineering | <ul style="list-style-type: none"> - requirement analysis - requirements feasibility assessment - disturbance quantification - error source identification and relevant numerical figures allocation to budgets | <ul style="list-style-type: none"> - analytical relationships and models - spreadsheet analysis tools - control CAD tools - simplified control, environment and sensors/actuators models |
| Design | <ul style="list-style-type: none"> - numerical trade studies in support of control architecture definition - numerical analysis to support control design - disturbance effects detailed analysis <ul style="list-style-type: none"> - stability - robustness - sensitivity to additional and/or parametric disturbances - performance against applicable requirements - control budget(s) numerical figures consolidation | <ul style="list-style-type: none"> - analytical relationships and models - spreadsheet analysis tools - 3D system model (if available) - control CAD tools - closed-loop simulation tools (including detailed control, environment and sensors/actuators models) - statistical methods and tools |
| Verification | <ul style="list-style-type: none"> - performance analysis verification (all-simulated environment) - control system verification/validation (H/W-, S/W-, human-in-the-loop test environment) - in-flight validation - support to payload data evaluation | <ul style="list-style-type: none"> - closed-loop simulations test-beds <ul style="list-style-type: none"> - all simulated - with control H/W-, S/W- and human-in-the loop - telemetry data processing tools - control CAD tools |

Table 5-1: Contributions of Analysis to the CE Process

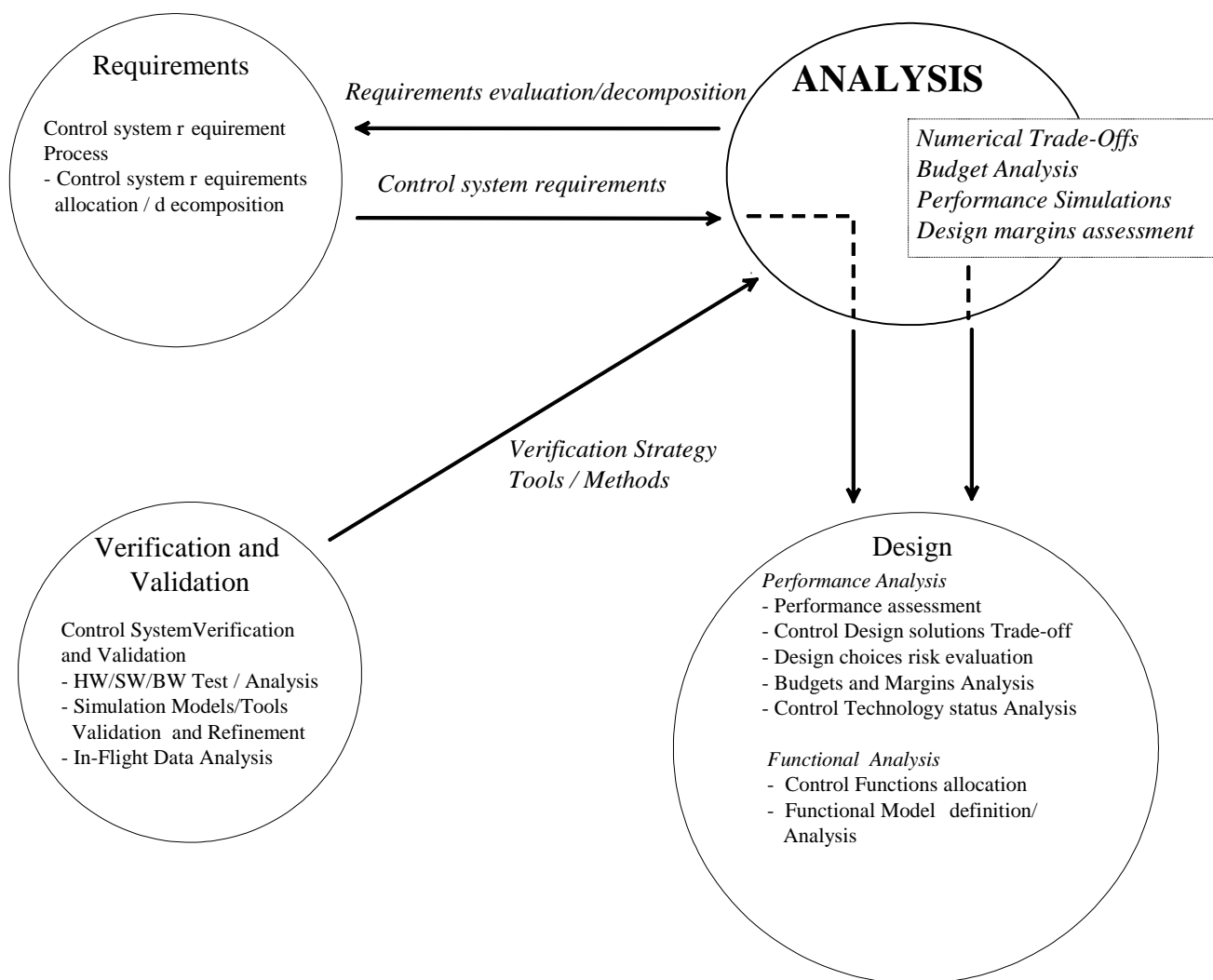


Figure 5-1: Analysis Contributions to the CE Process

5.3.2 Performance analysis

The scope of the analysis is to verify that the control system performance meet the control objectives generated by the requirement engineering process (see Figure 1-1).

- 5.3-1: For the performance assessment of the control system a mathematical model shall be developed.
- 5.3-2 A mathematical description of models shall be defined including fundamental assumptions and validity ranges.
- 5.3-3: The accuracy and the assumptions of the model shall be in accordance with the criteria established by the verification strategy derived from the mission and system definition.
- 5.3-4: The mathematical model shall be able to accurately predict the control system behaviour in the time domain (via simulation runs) and also allow input-output data processing.

5.3-5: The model shall be structured to support parametric analysis for trade-offs and optimisation of products selections.

5.3-6: The mathematical model shall be gradually refined during the project phases and its updates and improvements adequately traced.

5.3-7: The mathematical model of the control system shall include:

Model of the controlled plant: equation based kinematic and dynamical description of the plant under control (continuous time, discrete-time, hybrid, differential equations, state transition, nonlinearities etc.)

Model of the controller: H/W (analog compensator/filters), S/W (control algorithms, estimators / observers), state logic, supervisors, hybrid systems;

Sensors model in terms of: linearity, resolution, accuracy, noise, bandwidth/response time, delays

Actuators model in terms of: linearity, resolution, accuracy, work ranges, command rate, response time after receiving a (step) command, inherent time delays, noise

Model of the interaction of control system with the environment (e.g. disturbance model)

Signal conditioning within the control system: A/D converters sampling rates, quantization, D/A converters type, resolution, quantization interval

Model of control loop reference signals (setpoints) which may be the result of pre-processing

5.3-8 The mathematical model shall provide the necessary outputs for the performance evaluation (via post-processing).

5.3-9: The performance analysis shall assess the control system requirements fulfilment

Response to reference signals (setpoints)

Disturbance rejection: Assessment of the control system performance in the presence of internal disturbances (e.g. from sensors/actuators, controller) and environmental disturbances (e.g. gravity gradient, solar pressure)

5.3-10: The performance analysis shall address:

Stability Analysis: gain and phase margins of the control system

Control Law Sensitivity: robustness of the control law with respect to plant parameters uncertainty and drift.

5.3.3 Trade studies

5.3-11: Numerical Trade-offs shall be established by simulation of the control system performance respect to control objectives, with the aim of allowing evaluation of alternative control architectures, selection among different physical components, comparison of different candidate control law strategies.

5.3-12: TBD

5.3.4 Analysis tools and methods

- 5.3-13: Adequate analytical method and tools shall be adopted according to the different analysis task (e.g. control system requirement allocation, performance evaluation and trade-off).
- 5.3-14: The model shall be developed using well accepted S/W simulation packages.
- 5.3-15: Approaches
- Top/Down
 - Multi-layered, hierarchical
 - Simplified, conceptual
 - Analytical, equation based
 - Numerical computer simulation based
 - Hardware / Software in the loop
- 5.3-16: Tools
- Computer aided tools (CAD) (Matlab/Simulink, Matrix-X, MathCAD, Mathematica)
 - Functional modelling tools
 - Simplified (logical, conceptual, spreadsheet) models
- 5.3-17: Adequate methods and tools must be used at each stage of the development to perform analysis.
- 5.3-18: In early phases simplified control engineering models are used in combination with dedicated control analysis and control development tools. Model uncertainties can be taken into account assuring robustness of the design in a later phase. These control engineering models are often complementary to the detailed simulation models used for accurate simulation and verification of performances.
- 5.3-19: Simulation tools are required in Control Engineering for analysis, design and verification. These tools can be off-the-shelf or developed specifically for the programme at hand. In this later case, Control Engineering contributes to the specification, development and validation of such tool; this activity must be properly managed as part of the Control Engineering process.
- 5.3-20: Closed-loop simulations including models of the control system, sensors, actuators and control laws are used for analysis and verification of performances. As for other models and tools, the degree of accuracy of these simulations can increase during development according to the verification needs.
- 5.3-21: The accuracy of the mathematical models and tools, used for analysis performance predictions, but consolidated during the analysis phases shall be validated and verified according to a pre-specified verification plan.
- 5.3-22: The Usage of newly developed tools and models will imply proper justification configuration and validation activities.
- 5.3-23: The feasibility of adopting common simulation packages and tools within the frame of large projects shall be investigated, for increasing commonality among customer and sub-contractors to promote data sharing and exchange and increasing analysis effectiveness.

5.3.5 Analysis of requirements

- 5.3-24: Analysis activity shall contribute during the requirement engineering process in the decomposition of the high level mission objectives requirements. The method shall proceed from higher levels control objectives (customer needs) to lower levels, e.g. controller functions, physical components (sensors, actuators), human operators (BW).
- 5.3-25: With reference to the control system (see Figure 1-1), the requirements analysis engineering process (function) shall support in producing requirements on the controller functions, structure, and on the physical components attributes.
- 5.3-26: The tools utilised shall be operational analyst expertise, hierarchical methods, conceptual models , flow-charts, etc..

5.3.6 Budgets methods and margins

- 5.3-27: When budgets are needed, the methodology to consolidate these budgets need to be established as well as the margin philosophy applied to guarantee the robustness of the design. Budgets methodology and margin philosophy can evolve during the development according to the level of maturity of the control system.

5.4 Design and configuration

The design engineering process for CE consist of the design and development of

- ❑ preliminary control design concept(s) to support feasibility studies. This may not only be on paper but may also be done by functional model simulation.
- ❑ a preliminary control design defining the functional and physical architecture of the control system. Assessed functions have to be allocated to control hardware/control software and human operation on ground and onboard, during both preparation and utilisation, according to the operational requirements.
- ❑ a detailed control design defining the realisation of all components and interfaces within the controlled system.

The design is mainly defined in **Technical Specifications**, a **Design Justification File** and **in Interface Control Documentation**. This must be final at the CDR when a decision is to be taken to allow further development and start production. Results at the PDR must prove confidence in the architecture of the controlled system design with its major components.

Support from Control System Engineering is required for efficient organisation of the often complex design engineering process involving the different disciplines and components.

To reduce technical risks the CE design engineering process evidently makes use of simulators, and test tools. Costly design tools may also be needed. To reduce (cost) risks for the project, approach and planning should be included in a CE **Design Development and Verification** (DDV) plan. Final version must be provided at the PDR.

This chapter defines the control architecture design as a sequence of steps (functional control architecture, operational control architecture and physical control architecture). These steps should be in principle be executed sequentially but

- ❑ there will be the need of iterations and
- ❑ parts of steps may be omitted in case of system constraints (e.g. reuse of existing design or implementations)

5.4.1 Functional design

The functional design process is also called in the literature functional analysis. It consists in a resolution of control objectives into control system functions. This is usually achieved through a top/down procedure.

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

Previous Definitions (to be moved to definition of terms)

- ❑ **control mode:** temporary configuration of the control system composed of a number of functions implemented through a unique set of controller algorithms, sensors, actuators upon a given specific plant configuration to perform a set of control objectives.

- ❑ **control mode transitions**
- ❑ **control objectives** consist of
 - functional requirements
 - performance requirements
- ❑ **control function**
 - system level
 - "lower level"

New Definitions, Thierry, 29.05.2001 (to be moved to definition of terms)

- ❑ Control objectives : the goals which the control system must achieve. When expressed in quantitative terms they are referred to as control requirements.
- ❑ Control function : any of a group of related control actions (or activities) contributing to achieving some of the control objectives.
- ❑ Control mode : temporary operational configuration of the control system implemented through a unique set of sensors, actuators and controller algorithms (including FDIR algorithms?) acting upon a given plant configuration.
- ❑ Control mode transition : the passage or change from one control mode to another.

Requirements

- 5.4-1: CE shall define a functional design consisting of the control system functions (and sub-functions) required to meet the control objectives.

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

The functional design shall be done using systematic and well accepted methods and shall be compatible with the system functional analysis.

- 5.4-2: CE shall define the operational control architecture which consists of a set of modes and transitions between modes covering all possible 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: The operational control architecture shall be preferably presented in the form of block diagrams showing mode transitions and data flows.

- 5.4-4: For each control mode, the design shall identify
- the necessary functions
 - 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 mode
its contribution to the control objectives

5.4-5: The design shall identify the conditions for transitions between modes

starting conditions (previous mode & specific conditions),
when the transition occurs (trigger conditions)
end-conditions (subsequent mode & specific conditions)

5.4-6: CE shall check that operational/functional design covers all the control objectives

5.4.2 Physical control architecture

The physical control architecture is the ensemble of components (sensors, actuators, controller and plant realised by hardware, software or humans) which are used to realise 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 require interaction with other disciplines and for complex systems are expected to be performed in co-ordination with system engineering.

- 5.4-7: Control Engineering shall define a set of sensors which can meet all the control objectives in terms of observability, performances, redundancy.
- 5.4-8: Control Engineering shall contribute to the definition of a sensor configuration (sensor product and accommodation) It shall verify that the selected sensor configuration is compatible with the control system design.
- 5.4-9: Control Engineering shall define a set of actuators which can meet all the control objectives in terms of controllability, performances, redundancy.
- 5.4-10: Control Engineering shall contribute to the definition of an actuator configuration (actuator product and accommodation). It shall verify that the selected actuator configuration is compatible with the control system design.
- 5.4-11: Control Engineering shall check if the operational dynamic conditions of the system to be controlled are compatible with the selected configuration of sensors and actuators.
- 5.4-12: Control Engineering shall contribute to the design of the plant w.r.t. to the system dynamics and kinematics affecting the control performance. It shall verify that the selected plant configuration is compatible with the control system design.
- 5.4-13: Control Engineering shall contribute to the design of the electrical system architecture w.r.t. electrical interfaces affecting the control performance.
- 5.4-14: Control Engineering shall contribute to the onboard processing architecture w.r.t. processing capability, data rates, inputs/outputs, memory affecting the control performance.
- 5.4-15: 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, EOL) in particular due to environment conditions.
- 5.4-16: Control Engineering shall verify that the definition of interfaces with ground facilities, humans and/or with other space vehicles, if such are part of the system, allows to achieve the control objectives.

5.4.3 Controller design

The controller uses algorithms (mathematical or logical) to elaborate, from sensor measurements, commands to the actuators. These algorithms are designed to achieve the control objectives while being robust to uncertainties or predicted evolutions in the control system (controlled plant or control components). The control algorithms can be implemented in digital or analog form.

5.4-17: The controller design shall meet all control system performance requirements

Use of terms such as response time, settling time, bandwidth, RPE, APE, DPE, AME

Worst case performances, worst case parameters, worst case conditions

...

5.4-18: The controller design shall be robust in the face of uncertainties or predicted evolutions

Uncertainties in model properties used for controller design

Variations of process, sensor and actuators properties between B.O.L. and E.O.L.

...

5.4-19: The controller design shall be compatible with operational requirements such as

autonomy with respect to ground

observability from ground

...

5.4-20: The controller design shall be compatible of specific failures (in agreement with the system requirements)

reconfiguration

...

5.4.4 Configuration management and controller budgets

5.4-21: Inputs for system configuration management:

status of control performances

list of delivered control documents

...

5.4-22: Inputs for the control design during design, development and production:

delay budgets

mass and inertia budgets

mechanical eigenfrequencies which may be relevant

mechanical stiffness properties which may be relevant

...

5.4.5 Other topics

5.4-23: Guidelines deliverable control documents.

...

Section 5.4 to be updated and completed in the area of 'failure detection, isolation and recovery'.

5.5 Verification and validation

The CE verification process is the confirmation by examination and provision of objective evidence that specified requirements have been fulfilled (see ECSS-P-001).

The CE validation process is the confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled (see ECSS-P-001).

The Control Engineering verification/validation process is a part of the system verification/validation process and therefore shall be consistent with the verification requirements defined in ECSS-10A and ECSS-10-02A.

The CE verification already starts from the earliest phase when possible concepts are identified and one control system concept is selected. An important part of the CE 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 control system level. Finally, as not all control performances can be verified on ground, it may be required to perform additional verification in orbit.

5.5.1 Definition of control verification strategy

5.5-1: The CE verification process shall primarily

- verify that the control system will be able to achieve the required control objectives

- qualify the design of each part of the control system with respect to the applicable requirements

- verify that the hardware and software components of the control system comply with the qualified design and are acceptable for use

- confirm control system integrity and performances after particular steps of the project life cycle (pre-launch, in orbit)

5.5-2: The strategy of verification of the control system shall be defined in consistency with the system verification plan.

5.5-3: The CE verification strategy shall enable to demonstrate that all the control system requirements are met.

5.5-4: A plan for the verification and validation of the control system shall be developed and documented. It can be part of the system verification plan.

5.5-5: The effort for the verification of the control objectives shall be assessed according to the maturity and flight experience of the control system design.

5.5-6: The CE verification plan shall include

- the logic between the different verification levels related to control (component level, control system level, system level)
- the methods used to verify the control system requirements (reduced or full performance simulation, equipment level testing, open and closed loop testing with or without H/W-in-the-loop)
- the description of control system verification and validation activities
- the resources, responsibilities and schedule
- the description of the procedures and tools and facilities required for control system verification
- the model philosophy

5.5-7: The CE verification activities shall be phased in consistency with the lower levels (control system components) and upper levels (system level) verification activities.

5.5-8: When necessary, the strategy of validation of the models and tools used for the control system verification shall be included in the CE verification plan.

5.5.2 Preliminary verification of performance

5.5-9: To reduce risks, the CE verification process shall start early in the project to validate the control concepts and design as they are available.

5.5-10: The verification of critical features shall be performed during the design and development phases relying on simulation models or development models (prototypes).

5.5-11: The representativity and accuracy of the simulation models and tools used for the verification shall be validated. The process can be iterative according to the design maturity.

5.5.3 Final functional & performance verification

Level of detail depending on project status ...

5.5.3.1 Verification by analysis

5.5-12: The performances of the control system shall be demonstrated by closed loop analysis based on the use of system representative simulation models.

5.5-13: The control system performances shall be demonstrated in worst cases with respect to system dynamical and geometrical conditions, including FDIR resulting conditions.

5.5-14: The verification shall cover all control system modes and sensors/actuators operational configurations, including back-up configurations.

5.5.3.2 Verification with flight H/W and S/W

- 5.5-15: When applicable, numerical correctness of the control S/W on the target H/W (or emulator) shall be verified.
- 5.5-16: The CE verification process shall include as far as possible functional validation in closed loop tests with flight S/W and flight H/W models or flight representative models. At this stage control robustness investigations may be included.
- 5.5-17: The real sensors shall be stimulated as close as possible from the detectors by EGSE.
- 5.5-18: All modes transitions including FDIR mechanisms shall be tested and validated.

5.5.3.3 Acceptance verification (to be checked with 5.5.3.1 and 5.5.3.2)

- 5.5-19: The control engineering shall support acceptance for the control system H/W and S/W components.
- 5.5-20: The performances of the hardware components of the control system shall be verified. They shall be compliant with the control system performances requirements.
- 5.5-21: Acceptance tests shall be performed onto the control system based on open loop tests to verify:
- Flight H/W and S/W integration
 - Internal and external interfaces
 - Flight data base
- 5.5-22: After final integration, polarity of the sensors and actuators shall be verified.

5.5.4 In orbit validation

- 5.5-23: When in-orbit validation is required, ground observability on the control system shall be sufficient to enable verification.

5.6 Operations

5.6-1: TBD

5.6-2: TBD

A mode of Operation describes the circumstantial fashion (mostly w.r.t. the extent of human involvement) in which particular Functions are to be performed. For instance, the mode of Operation specifies the allocation of control Functions among humans (Brainware) and machines (hardware and software) of different specialisation and skill level and at different sites (e.g. in the Ground Segment or in the Space Segment). The mode of Operation says BY WHOM a Function is performed, but not HOW (see Implementation).

Important task of Control System Engineering during the O-A phase is the Activity Analysis defining control activities to be performed in terms of Mission, Tasks and Actions.

Important task of Control System Engineering during the B phase is the Operational Requirements Analysis allocating control system functions:

- ☐ WHEN do the control functions have to be performed ?
- ☐ BY WHOM ? : by hardware, software or humans ?
- ☐ WHERE ? : on ground or on board ?

TBW : possible contribution, support of Control Engineering to

- ☐ Development of Ground Support Equipment
- ☐ Operations Preparation
- ☐ Operations training
- ☐ Operations Validation
- ☐ Operations Execution
- ☐ In line with ECSS-E-00 "Policy and Principles", Section Operations.

TBW better: CE must specify control functions required on ground in connection with the control system in orbit. CE must also specify possible need for verification of control system requirements in orbit. CE shall specify measurement data (part of telemetry) to be send to ground for on-line or off line processing. Such data are needed to support commissioning of the control system and to enable in-orbit verification.

Annexes: Document Requirements Definitions (DRD)

- ☐ Document requirements definitions for all documents identified in chapter 5.